Fortifying Software Resilience:

A Roadmap for Mitigating Risks in the Evolving SDV Landscape

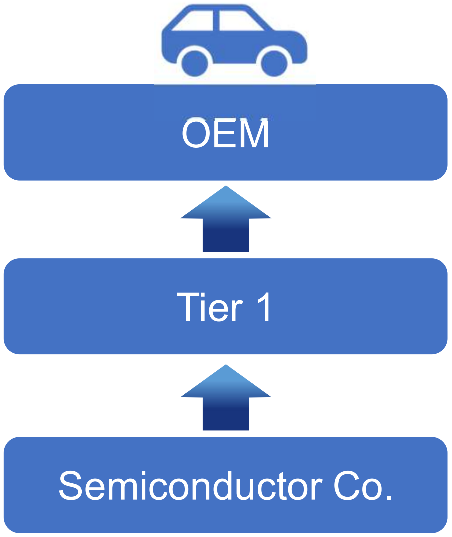
Ian Chu

VicOne

ian_chu@vicone.com

Automotive Ecosystem Evolved

TIERED

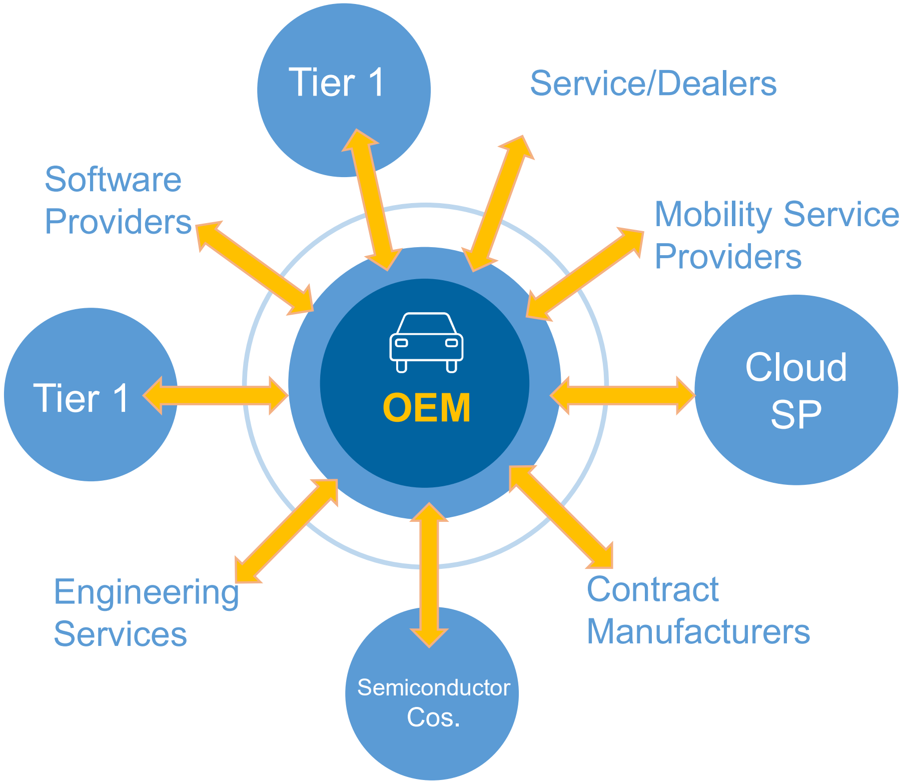


OEM

Tier 1

Semiconductor Co.

BIDIRECTIONAL & INTERCONNECTED



Tier 1

Service/Dealers

Software Providers

Mobility Service Providers

Tier 1

OEM

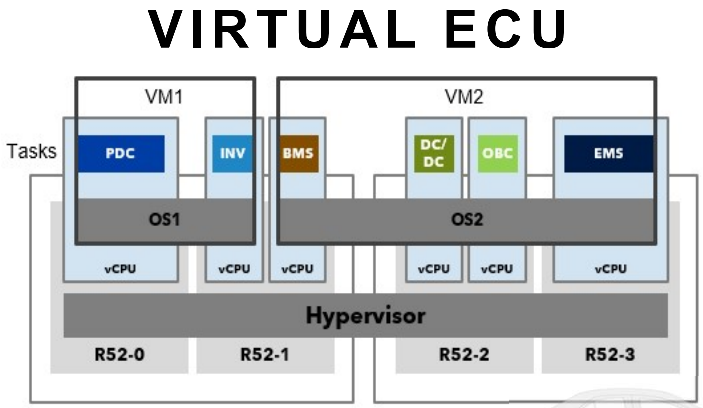
Cloud SP

Engineering Services

Contract Manufacturers

Semiconductor Cos.

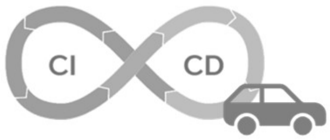
Virtual ECU Advancements fuel SDV



NXP Qualcomm

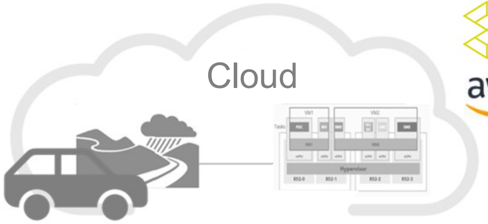
Picture Credit: NXP

✓ **Implementing CI/CD** for
accelerated vehicle design process



✓ **Realizing Updateable Local Systems**
for advanced software integration

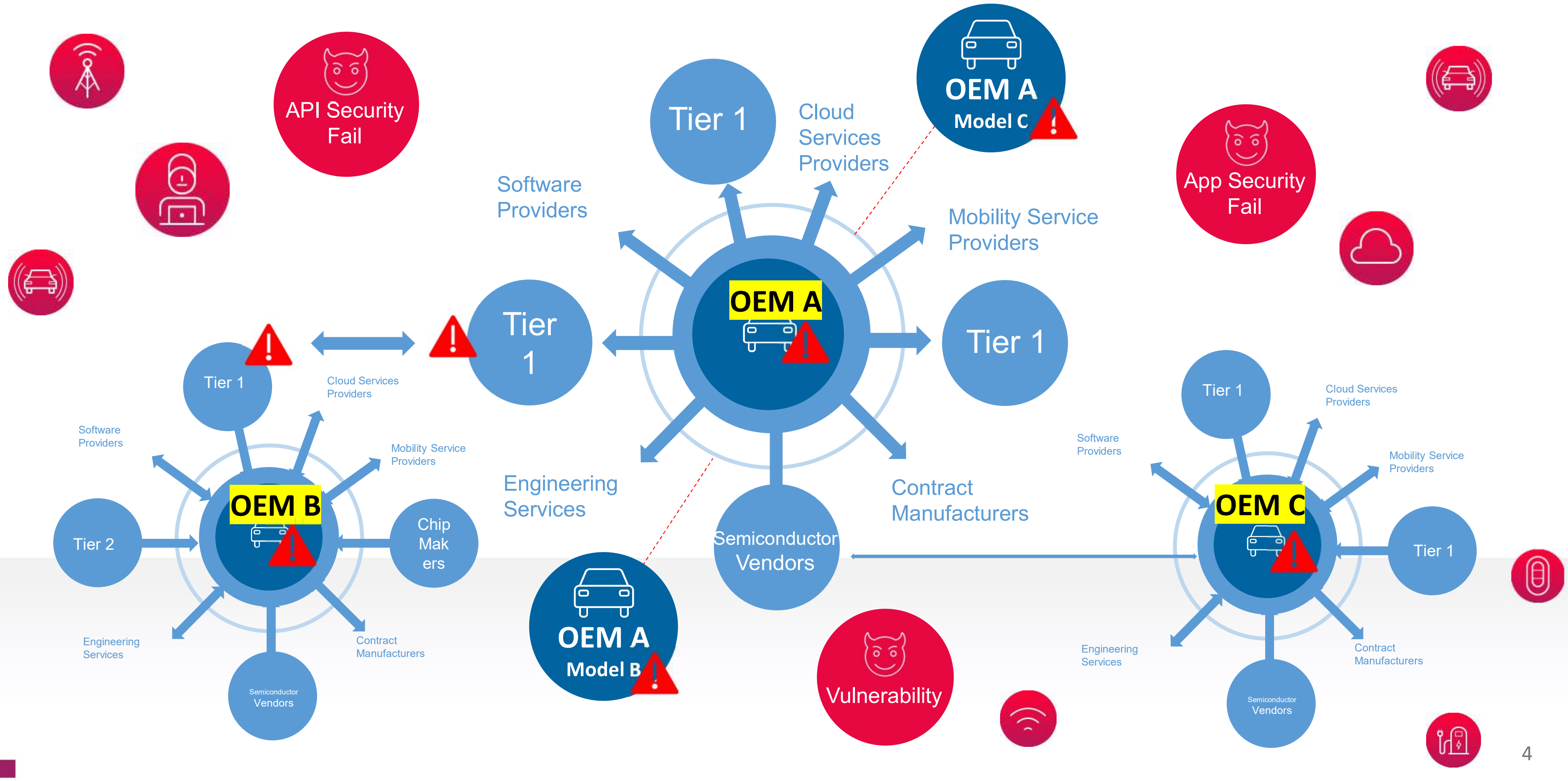
✓ **Feasibility of Digital Twin** for
system integration simulation



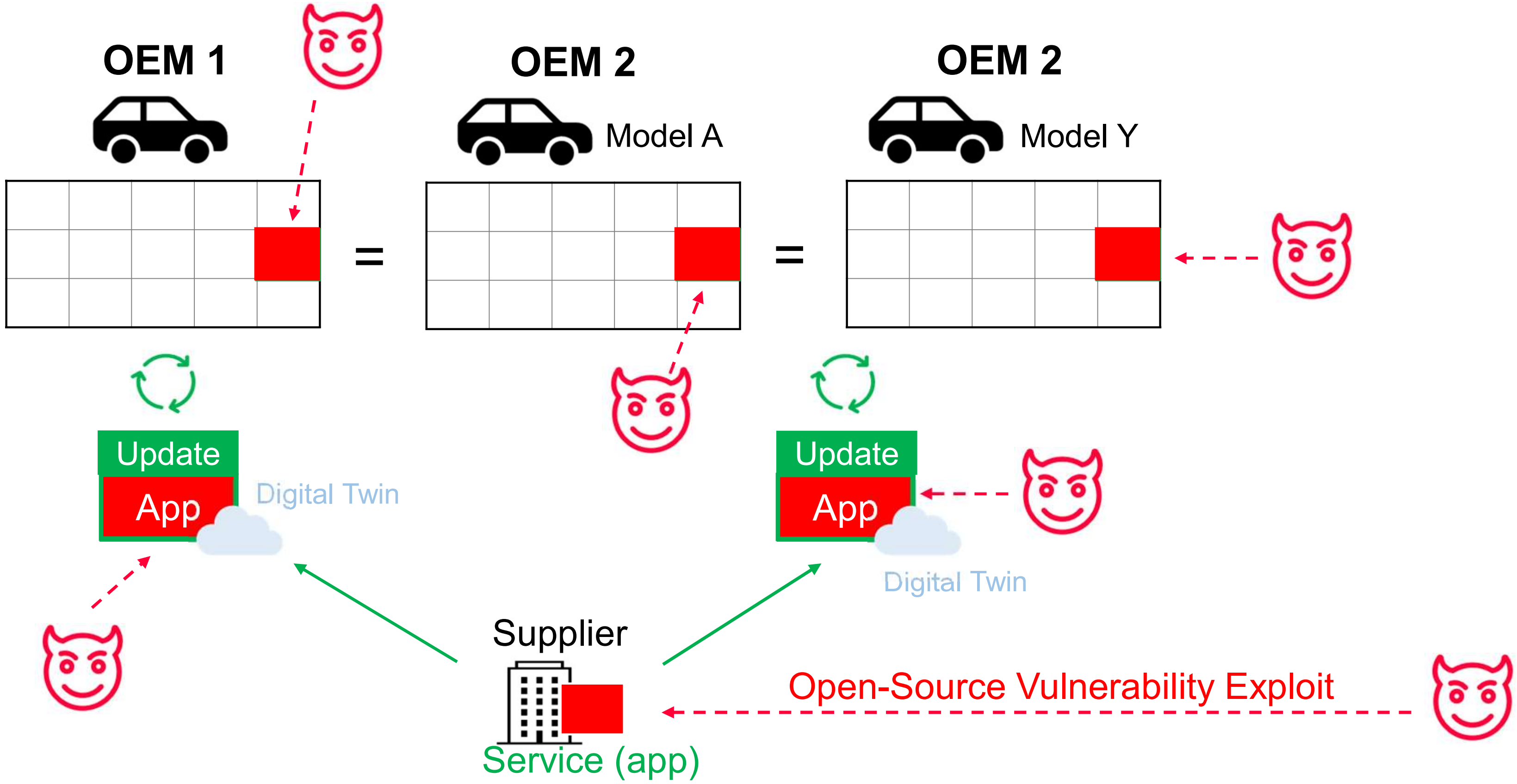
SOAFEE

aws

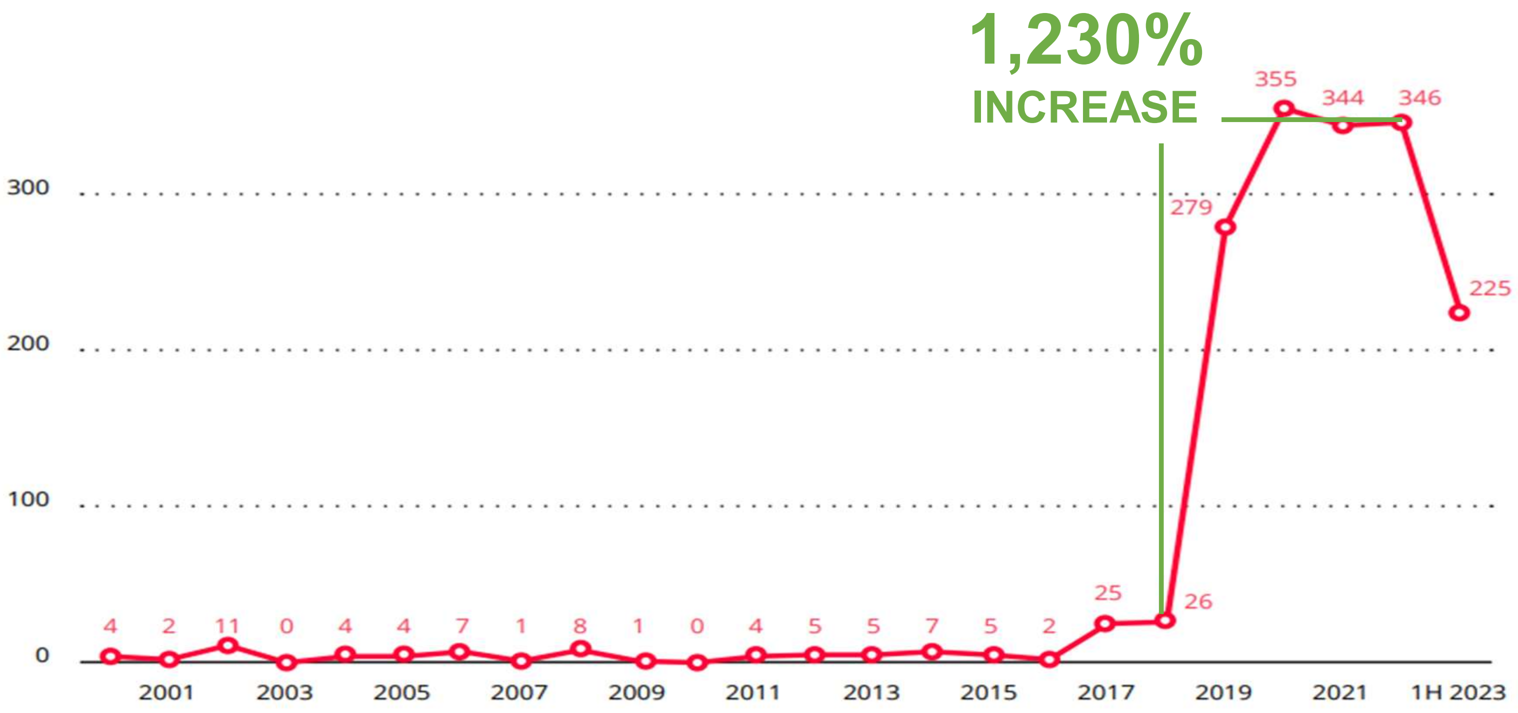
Threat landscape – Wider and more open



Software Risks Fueling **Supply Chain Attacks**



Growing Rapidly:
Hundreds of Reported Automotive Vulnerabilities



1,230%
INCREASE

Effects of Exposed Vulnerabilities in Automotive Systems, for example: Data theft/harvest, Device hijack, Device malfunction, Loss of system/service availability, Network host services disabled….

Source: VicOne and NVD database

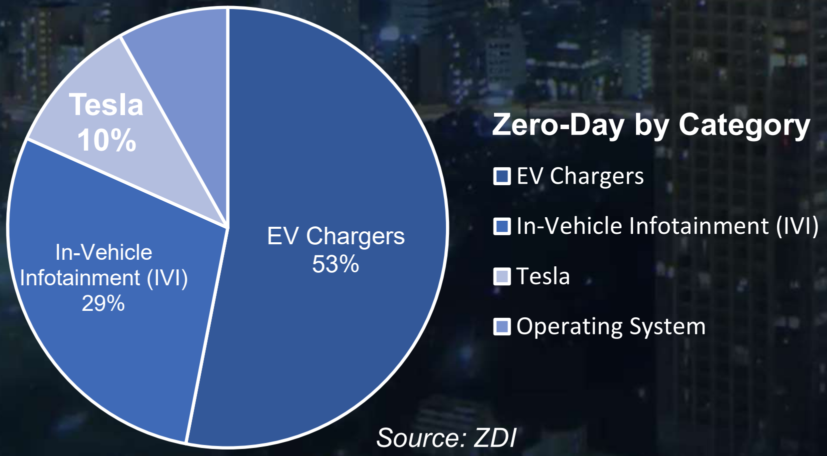
https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/rising-security-weaknesses-in-the-automotive-industry-and-what-it-can-do-on-the-road-ahead

Jan. 24- 26, 2024

Pwn2Own Automotive: The **first-ever** Automotive Hacking Contests

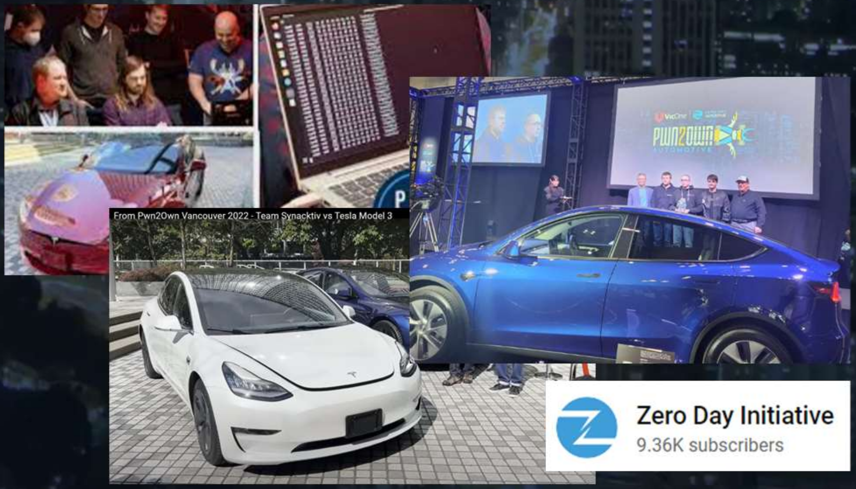
17 white hat hacker team, nine countries participated, over 50 entries remotely and on-site across four categories

49 unique **zero-day vulnerabilities** for automotive industry in **3 days**



Source: ZDI

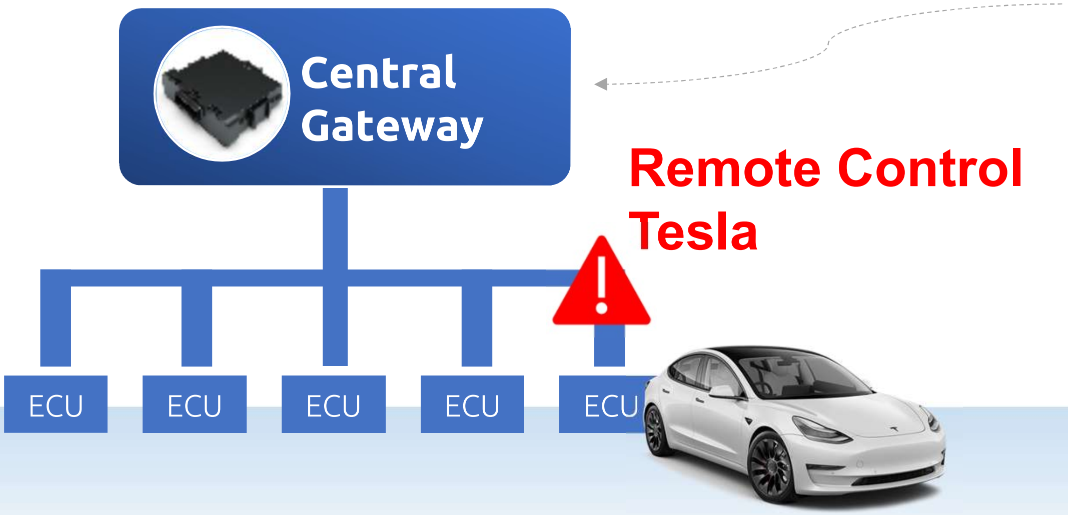
Tesla has been our partner for over 5 years


From Pwn2Own Vancouver 2022 - Team Synacktiv vs Tesla Model 3
Zero Day Initiative
9.36K subscribers

Disclosed **13 zero-day** vulnerabilities related to Tesla since 2017

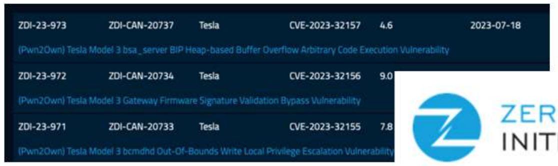
Source: https://www.youtube.com/watch?v=ZUs98Z-plpY

Scary Zero Day Vulnerabilities:
Attackers Can *Remote* Control Tesla



3 Actual Tesla Zero-Day Vulnerabilities' Impact

1. Remote Vulnerability Attack (ZDI-23-973)
2. Privilege Escalation (ZDI-23-971)
3. Validation Bypass (ZDI-23-972)



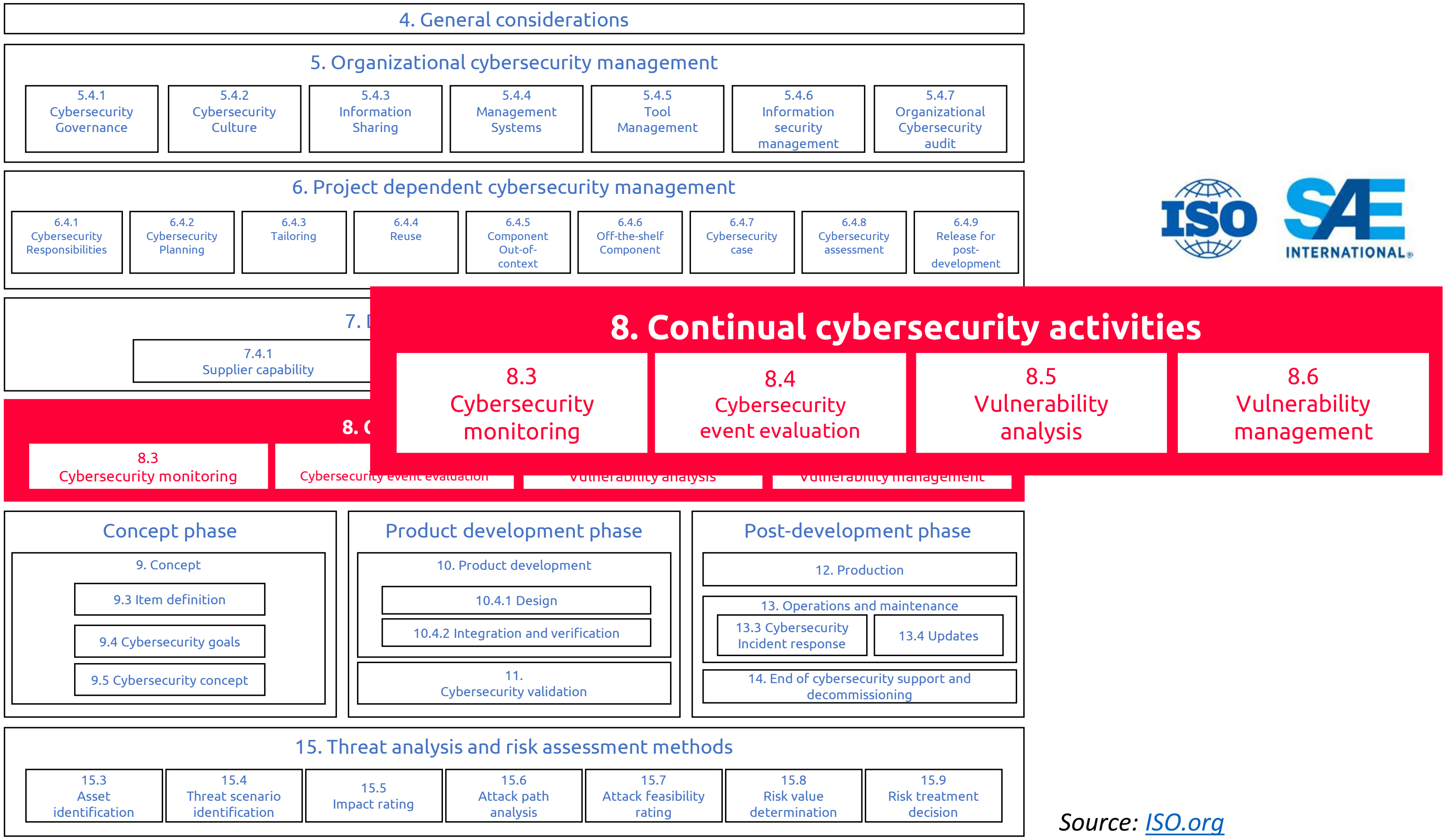
ZDI-23-973	ZDI-CAN-20737	Tesla	CVE-2023-32157	4.6	2023-07-18
(Pwn2Own) Tesla Model 3 bsa_server BIP Heap-based Buffer Overflow Arbitrary Code Execution Vulnerability					
ZDI-23-972	ZDI-CAN-20734	Tesla	CVE-2023-32156	9.0	
(Pwn2Own) Tesla Model 3 Gateway Firmware Signature Validation Bypass Vulnerability					
ZDI-23-971	ZDI-CAN-20733	Tesla	CVE-2023-32155	7.8	
(Pwn2Own) Tesla Model 3 bcmdhd Out-Of-Bounds Write Local Privilege Escalation Vulnerability					

ZERO DAY INITIATIVE

Vulnerabilities Management

Challenge SDV CI/CD process

ISO/SAE 21434 Requires **Vulnerability Management**



4. General considerations

5. Organizational cybersecurity management

5.4.1 Cybersecurity Governance

5.4.2 Cybersecurity Culture

5.4.3 Information Sharing

5.4.4 Management Systems

5.4.5 Tool Management

5.4.6 Information security management

5.4.7 Organizational Cybersecurity audit

6. Project dependent cybersecurity management

6.4.1 Cybersecurity Responsibilities

6.4.2 Cybersecurity Planning

6.4.3 Tailoring

6.4.4 Reuse

6.4.5 Component Out-of-context

6.4.6 Off-the-shelf Component

6.4.7 Cybersecurity case

6.4.8 Cybersecurity assessment

6.4.9 Release for post-development

7.

7.4.1 Supplier capability

8. C

8.3 Cybersecurity monitoring

Cybersecurity event evaluation

Vulnerability analysis

Vulnerability management

8. Continual cybersecurity activities

8.3 Cybersecurity monitoring

8.4 Cybersecurity event evaluation

8.5 Vulnerability analysis

8.6 Vulnerability management

Concept phase

9. Concept

9.3 Item definition

9.4 Cybersecurity goals

9.5 Cybersecurity concept

Product development phase

10. Product development

10.4.1 Design

10.4.2 Integration and verification

11. Cybersecurity validation

Post-development phase

12. Production

13. Operations and maintenance

13.3 Cybersecurity Incident response

13.4 Updates

14. End of cybersecurity support and decommissioning

15. Threat analysis and risk assessment methods

15.3 Asset identification

15.4 Threat scenario identification

15.5 Impact rating

15.6 Attack path analysis

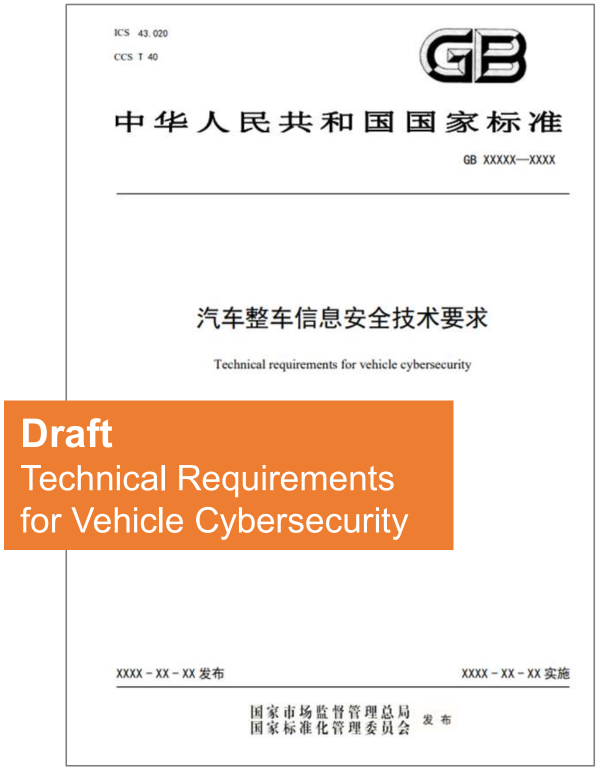
15.7 Attack feasibility rating

15.8 Risk value determination

15.9 Risk treatment decision

Source: *ISO.org*

Take effect in 2026:
New GB Standard Will Require **Vulnerability Management**



ICS 43.020
CCS T 40

中华人民共和国国家标准

GB XXXXX—XXXX

汽车整车信息安全技术要求

Technical requirements for vehicle cybersecurity

XXXX－XX－XX 发布　　XXXX－XX－XX 实施

国家市场监督管理总局
国家标准化管理委员会　发布

Draft
Technical Requirements
for Vehicle Cybersecurity

Take effect on Jan. 1, 2026

5.2.4 应建立针对车辆的网络攻击、网络威胁和漏洞的监测、响应及上报流程
Establishment of monitoring, response, and reporting process for cyberattacks, cyber threats, and vulnerabilities targeting vehicles

5.2.4 (e) 应建立确保对网络攻击、网络威胁和漏洞进行持续监控的流程
Process should be established to ensure **continuous monitoring of vulnerabilities**, cyberattacks, and cyber threats

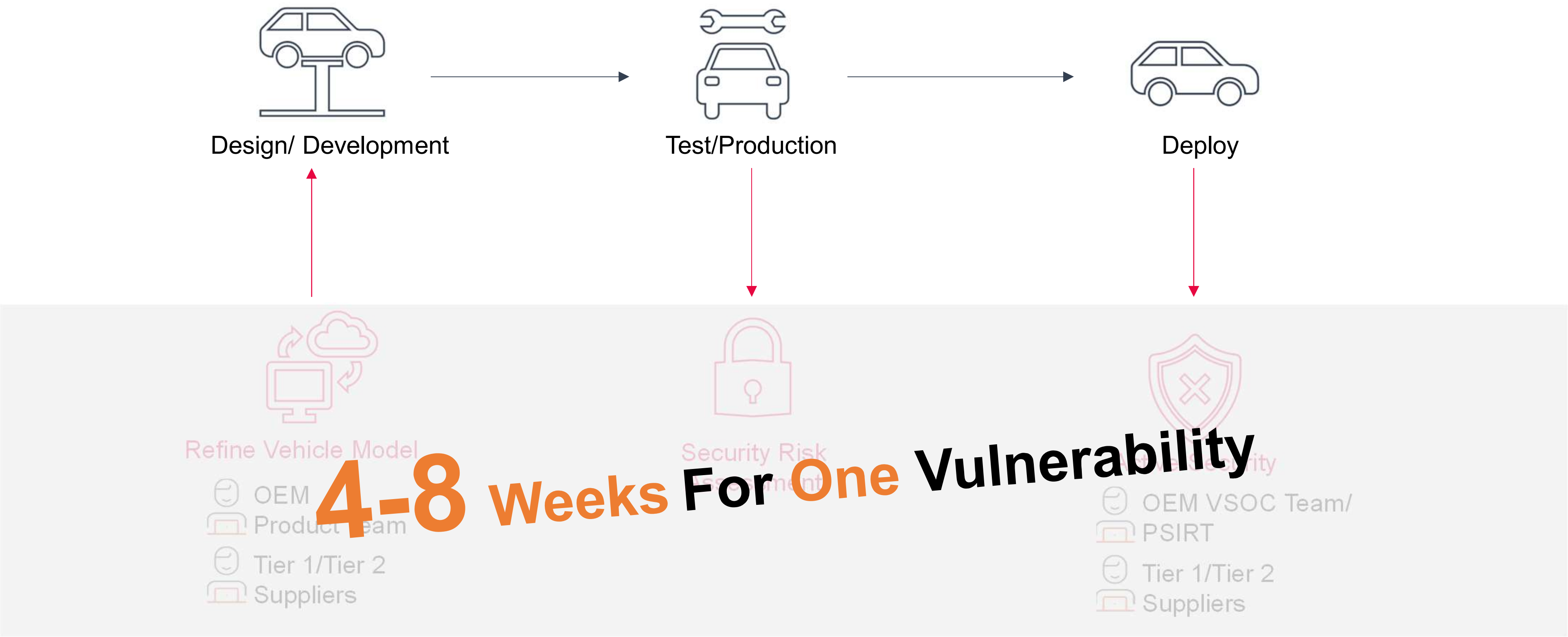
9.1.2 车载软件升级系统应不存在由权威漏洞平台 6 个月前公布且未经处置的高危及以上的安全漏洞
The vehicle software must **not contain high-risk vulnerabilities** disclosed by authoritative vulnerability databases over 6 months ago without resolution.

A.6.1.2 (a) 使用漏洞扫描工具对车载软件升级系统进行漏洞扫描测试
Conduct vulnerability scanning on the vehicle software by using vulnerability scanning tools.

A.6.1.2 (b) 对照企业提交的漏洞处置方案清单，确认企业提交的漏洞处置方案清单中是否覆盖该漏洞
Cross-reference the **list of vulnerability** mitigation plans submitted by the enterprise to verify if the submitted plans cover the identified vulnerability.

Source: https://members.wto.org/crnattachments/2023/TBT/CHN/23_11189_00_x.pdf

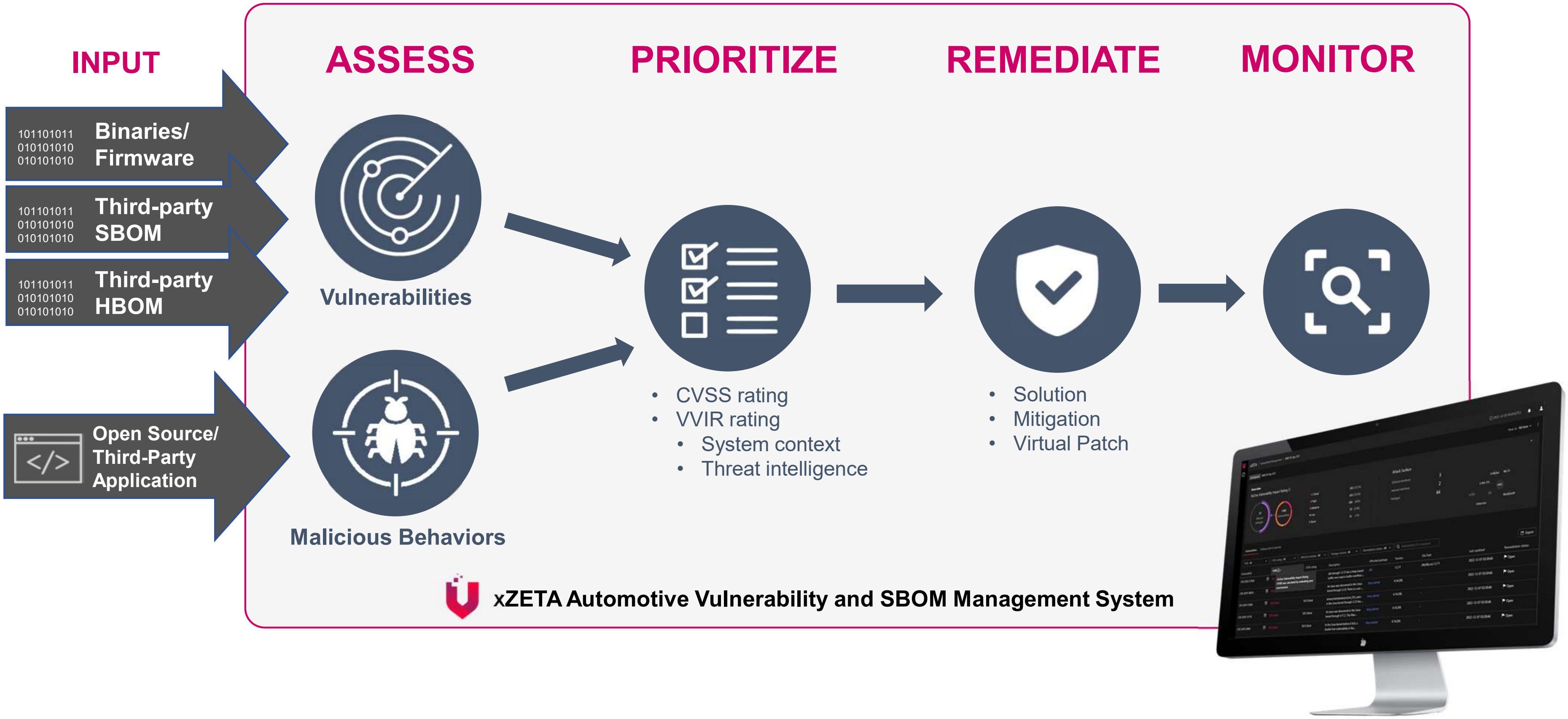
Challenging to Effectively Handle Vulnerability Risks on a **Large Scale**



4-8 Weeks For One Vulnerability

How do we keep up with the **rapidly evolving** development scenarios?

Manage Vulnerabilities in One Place, Automatically



INPUT

101101011
010101010
010101010
Binaries/
Firmware

101101011
010101010
010101010
Third-party
SBOM

101101011
010101010
010101010
Third-party
HBOM

Open Source/
Third-Party
Application

ASSESS

Vulnerabilities

Malicious Behaviors

PRIORITIZE

- CVSS rating
- VVIR rating
  - System context
  - Threat intelligence

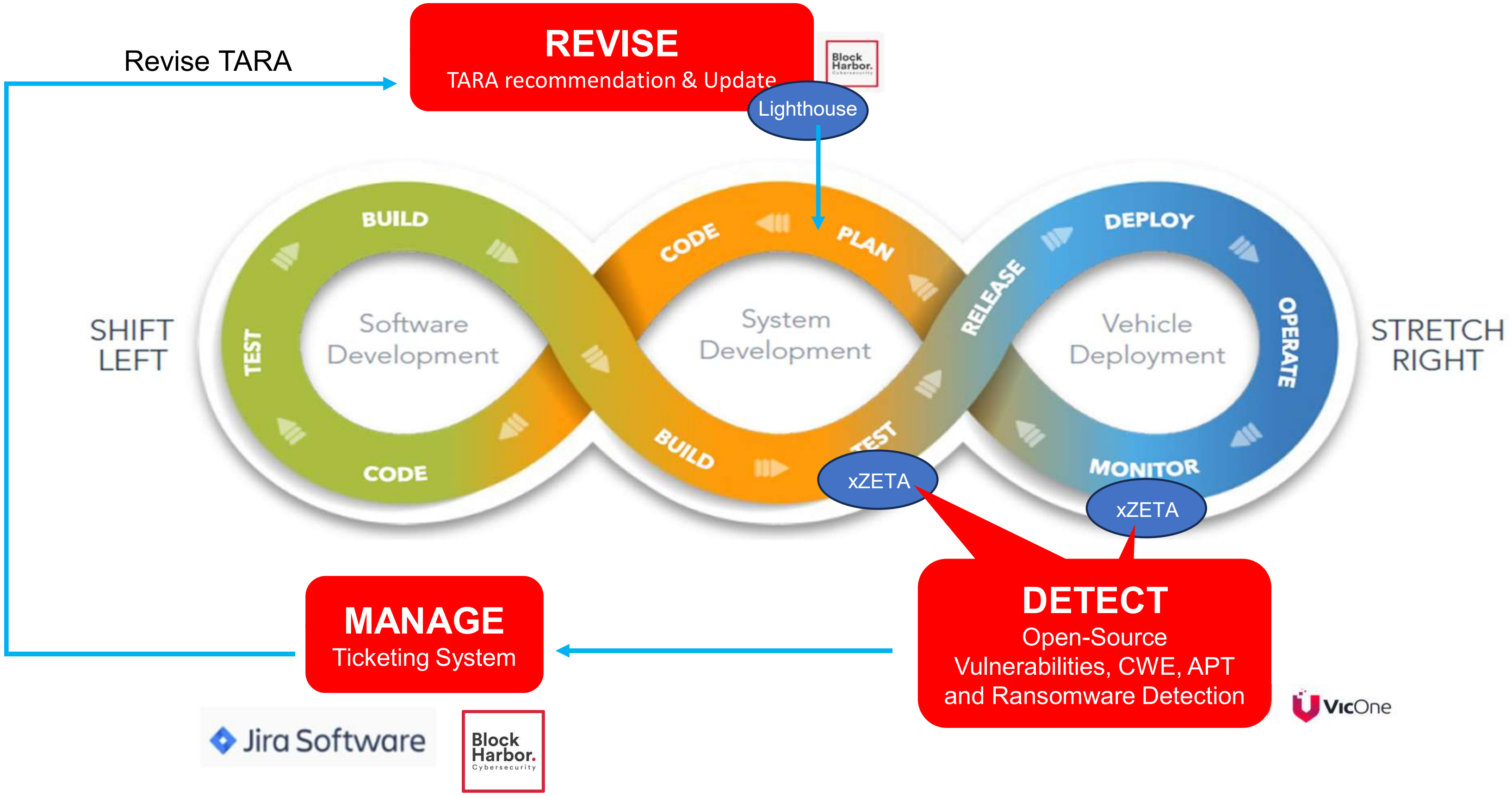
REMEDIATE

- Solution
- Mitigation
- Virtual Patch

MONITOR

xZETA Automotive Vulnerability and SBOM Management System

CI/CD Integration: Enhances Operational Efficiency



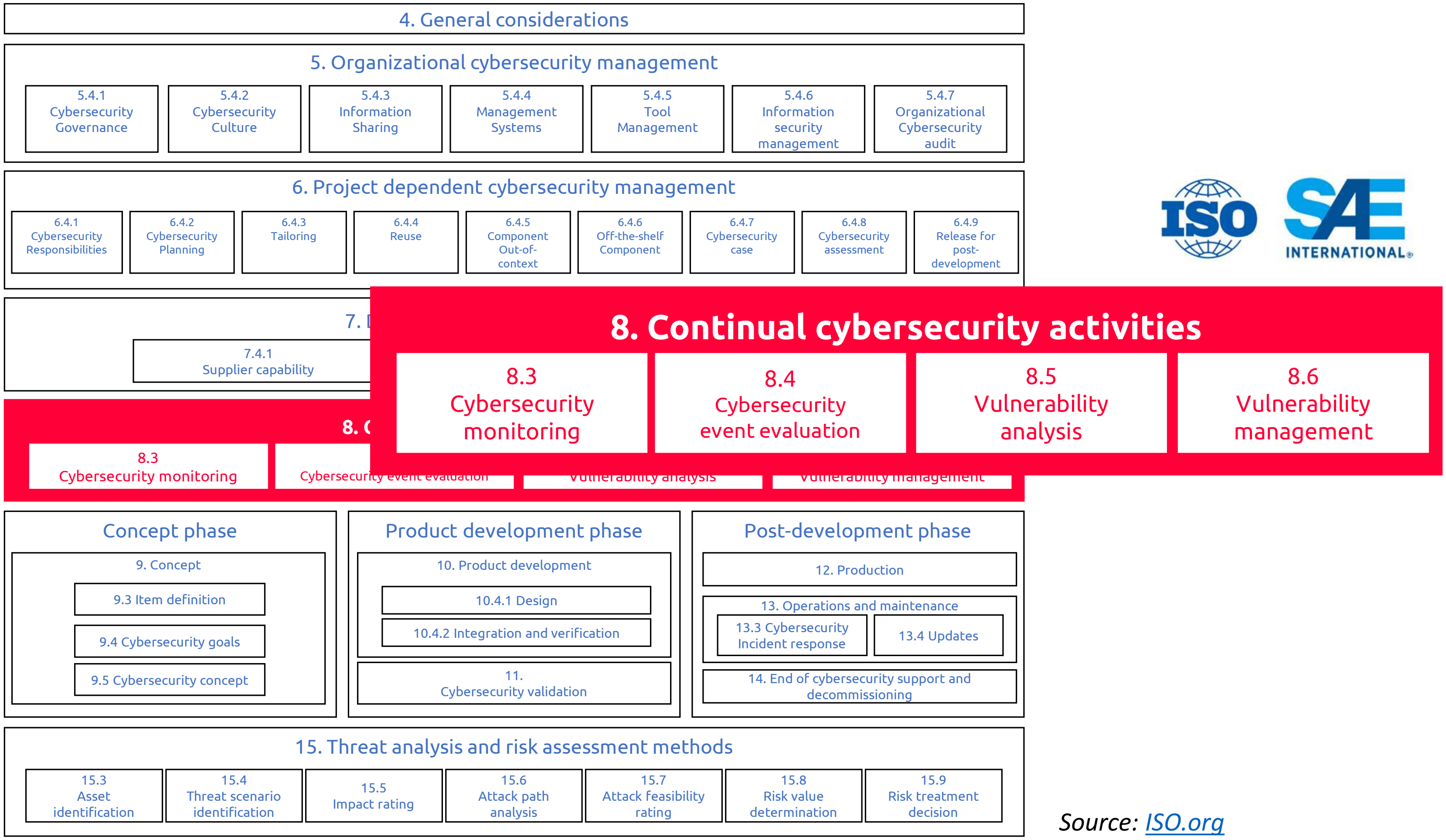
Revise TARA

REVISE
TARA recommendation & Update

MANAGE
Ticketing System

DETECT
Open-Source
Vulnerabilities, CWE, APT
and Ransomware Detection

How xZETA Can Help



4. General considerations

5. Organizational cybersecurity management

5.4.1 Cybersecurity Governance

5.4.2 Cybersecurity Culture

5.4.3 Information Sharing

5.4.4 Management Systems

5.4.5 Tool Management

5.4.6 Information security management

5.4.7 Organizational Cybersecurity audit

6. Project dependent cybersecurity management

6.4.1 Cybersecurity Responsibilities

6.4.2 Cybersecurity Planning

6.4.3 Tailoring

6.4.4 Reuse

6.4.5 Component Out-of-context

6.4.6 Off-the-shelf Component

6.4.7 Cybersecurity case

6.4.8 Cybersecurity assessment

6.4.9 Release for post-development

7. D

7.4.1 Supplier capability

8. C

8.3 Cybersecurity monitoring

Cybersecurity event evaluation

Vulnerability analysis

Vulnerability management

8. Continual cybersecurity activities

8.3 Cybersecurity monitoring

8.4 Cybersecurity event evaluation

8.5 Vulnerability analysis

8.6 Vulnerability management

Concept phase

9. Concept

9.3 Item definition

9.4 Cybersecurity goals

9.5 Cybersecurity concept

Product development phase

10. Product development

10.4.1 Design

10.4.2 Integration and verification

11. Cybersecurity validation

Post-development phase

12. Production

13. Operations and maintenance

13.3 Cybersecurity Incident response

13.4 Updates

14. End of cybersecurity support and decommissioning

15. Threat analysis and risk assessment methods

15.3 Asset identification

15.4 Threat scenario identification

15.5 Impact rating

15.6 Attack path analysis

15.7 Attack feasibility rating

15.8 Risk value determination

15.9 Risk treatment decision

ISO

SAE INTERNATIONAL

Source: ISO.org

8. Continual cybersecurity activities

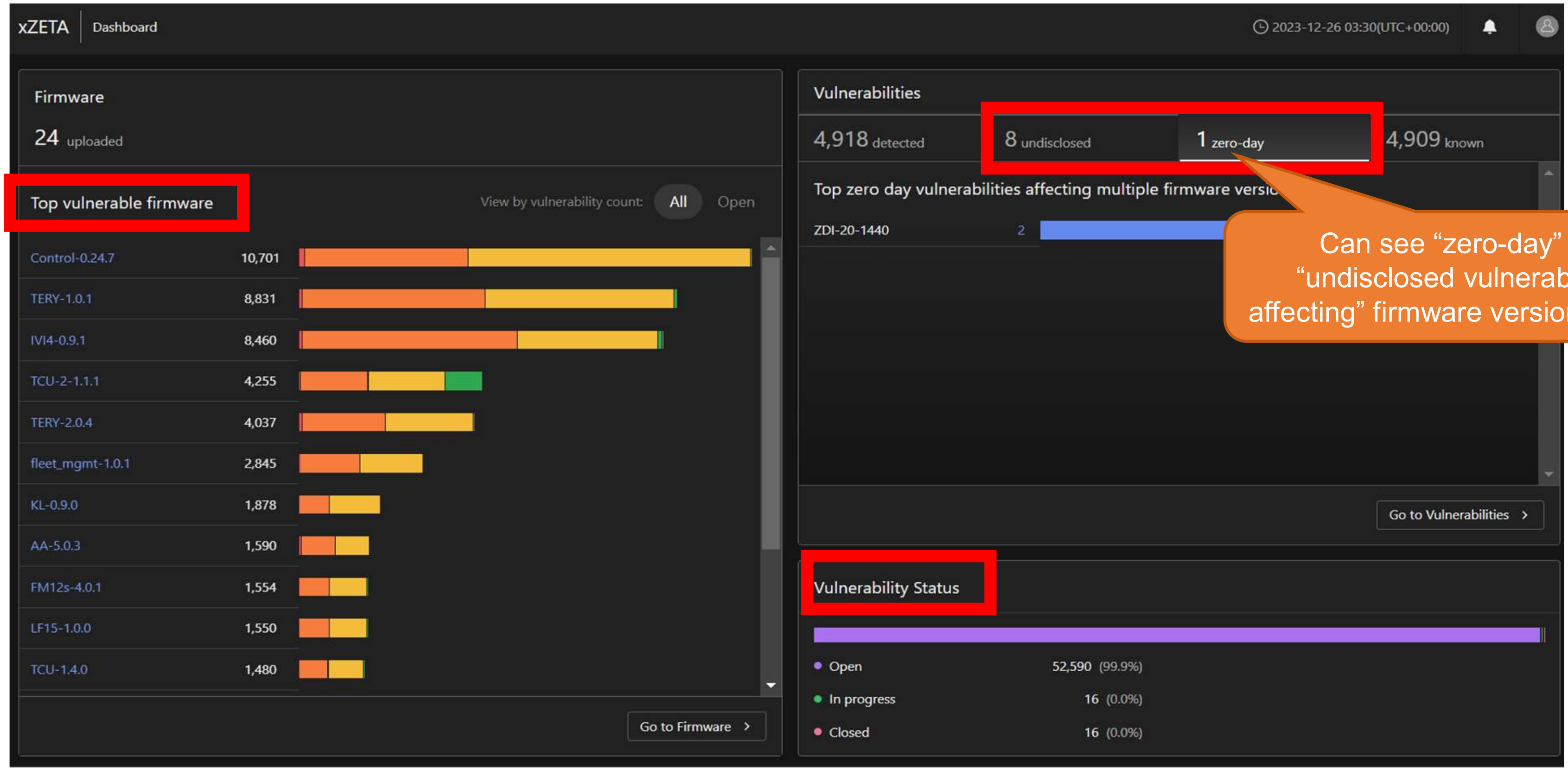
8.3 Cybersecurity monitoring | 8.4 Cybersecurity event evaluation | 8.5 Vulnerability analysis | 8.6 Vulnerability management

10. Product development

10.4.1 Design

10.4.2 Integration and verification

When a new vulnerability is disclosed, we can first overview the vulnerability status through the dashboard.



xZETA | Dashboard — 2023-12-26 03:30(UTC+00:00)

Firmware

24 uploaded

Top vulnerable firmware — View by vulnerability count: All | Open

Control-0.24.7	10,701
TERY-1.0.1	8,831
IVI4-0.9.1	8,460
TCU-2-1.1.1	4,255
TERY-2.0.4	4,037
fleet_mgmt-1.0.1	2,845
KL-0.9.0	1,878
AA-5.0.3	1,590
FM12s-4.0.1	1,554
LF15-1.0.0	1,550
TCU-1.4.0	1,480

Go to Firmware >

Vulnerabilities

4,918 detected | 8 undisclosed | 1 zero-day | 4,909 known

Top zero day vulnerabilities affecting multiple firmware versic

ZDI-20-1440	2

Go to Vulnerabilities >

Vulnerability Status

● Open	52,590	(99.9%)
● In progress	16	(0.0%)
● Closed	16	(0.0%)

Can see “zero-day” & “undisclosed vulnerability affecting” firmware versions here

8. Continual cybersecurity activities

8.3 Cybersecurity monitoring

8.4 Cybersecurity event evaluation`

8.5 Vulnerability analysis

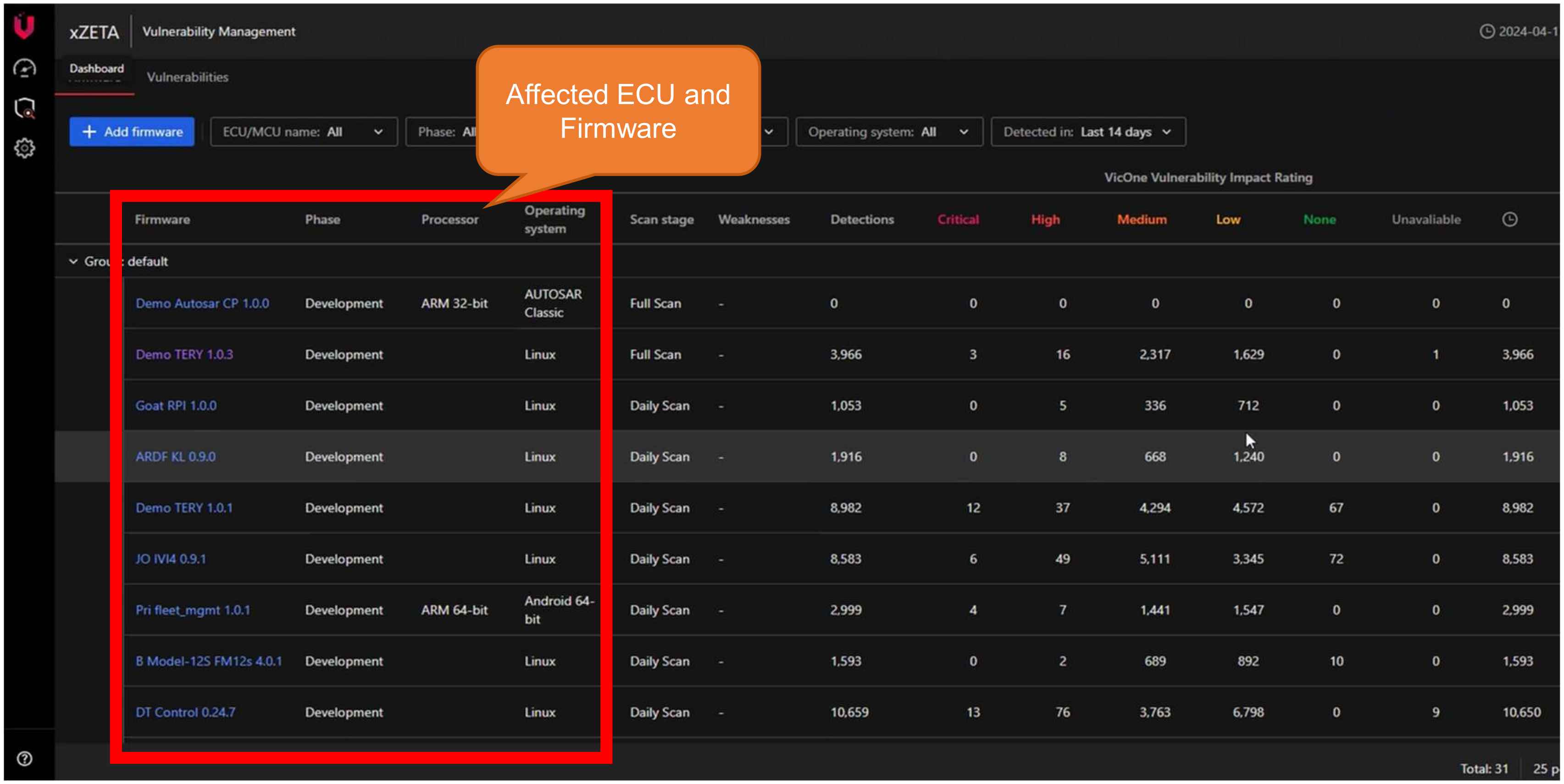
8.6 Vulnerability management

10. Product development

10.4.1 Design

10.4.2 Integration and verification

Through the ECU view, we can quickly confirm which products are affected by reported vulnerabilities.



ECU/MCU name: All | Phase: All | Operating system: All | Detected in: Last 14 days

Affected ECU and Firmware

VicOne Vulnerability Impact Rating

Group: default

Firmware	Phase	Processor	Operating system	Scan stage	Weaknesses	Detections	Critical	High	Medium	Low	None	Unavaliable	🕒
Demo Autosar CP 1.0.0	Development	ARM 32-bit	AUTOSAR Classic	Full Scan	-	0	0	0	0	0	0	0	0
Demo TERY 1.0.3	Development		Linux	Full Scan	-	3,966	3	16	2,317	1,629	0	1	3,966
Goat RPI 1.0.0	Development		Linux	Daily Scan	-	1,053	0	5	336	712	0	0	1,053
ARDF KL 0.9.0	Development		Linux	Daily Scan	-	1,916	0	8	668	1,240	0	0	1,916
Demo TERY 1.0.1	Development		Linux	Daily Scan	-	8,982	12	37	4,294	4,572	67	0	8,982
JO IVI4 0.9.1	Development		Linux	Daily Scan	-	8,583	6	49	5,111	3,345	72	0	8,583
Pri fleet_mgmt 1.0.1	Development	ARM 64-bit	Android 64-bit	Daily Scan	-	2,999	4	7	1,441	1,547	0	0	2,999
B Model-12S FM12s 4.0.1	Development		Linux	Daily Scan	-	1,593	0	2	689	892	10	0	1,593
DT Control 0.24.7	Development		Linux	Daily Scan	-	10,659	13	76	3,763	6,798	0	9	10,650

Total: 31 | 25 p

8. Continual cybersecurity activities

8.3 Cybersecurity monitoring

8.4 Cybersecurity event evaluation

8.5 Vulnerability analysis

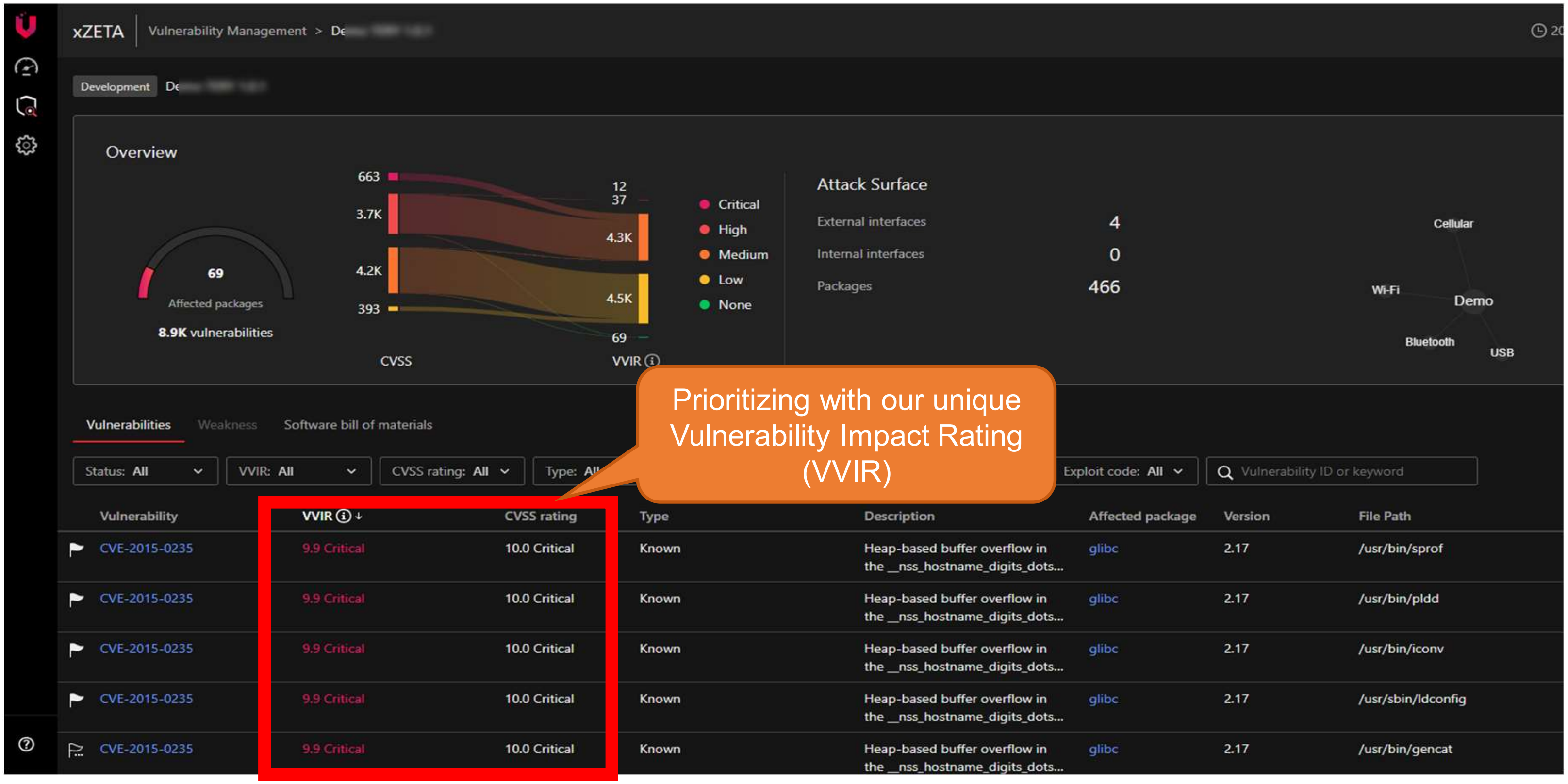
8.6 Vulnerability management

10. Product development

10.4.1 Design

10.4.2 Integration and verification

Leverage impact rating, we can assess the severity of this vulnerability on the products, prioritizing mitigation resource.



Attack Surface

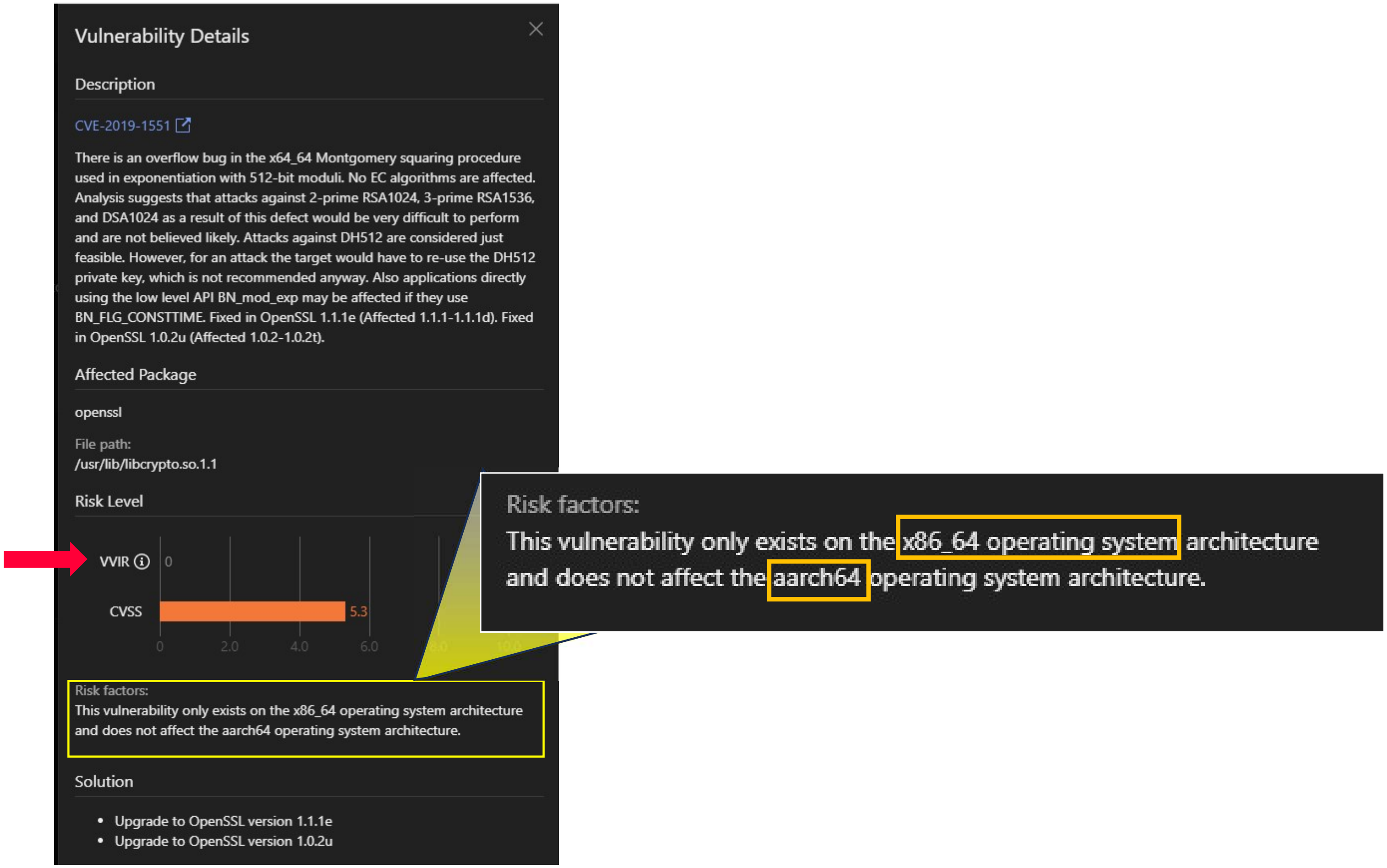
External interfaces	4
Internal interfaces	0
Packages	466

Status: All | VVIR: All | CVSS rating: All | Type: All | Exploit code: All | Vulnerability ID or keyword

Vulnerability	VVIR ↓	CVSS rating	Type	Description	Affected package	Version	File Path
CVE-2015-0235	9.9 Critical	10.0 Critical	Known	Heap-based buffer overflow in the __nss_hostname_digits_dots...	glibc	2.17	/usr/bin/sprof
CVE-2015-0235	9.9 Critical	10.0 Critical	Known	Heap-based buffer overflow in the __nss_hostname_digits_dots...	glibc	2.17	/usr/bin/pldd
CVE-2015-0235	9.9 Critical	10.0 Critical	Known	Heap-based buffer overflow in the __nss_hostname_digits_dots...	glibc	2.17	/usr/bin/iconv
CVE-2015-0235	9.9 Critical	10.0 Critical	Known	Heap-based buffer overflow in the __nss_hostname_digits_dots...	glibc	2.17	/usr/sbin/ldconfig
CVE-2015-0235	9.9 Critical	10.0 Critical	Known	Heap-based buffer overflow in the __nss_hostname_digits_dots...	glibc	2.17	/usr/bin/gencat

Prioritizing with our unique Vulnerability Impact Rating (VVIR)

Precise Prioritization - Practical Examples



Vulnerability Details

Description

CVE-2019-1551

There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u (Affected 1.0.2-1.0.2t).

Affected Package

openssl

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

Risk Level

Risk factors:
This vulnerability only exists on the x86_64 operating system architecture and does not affect the aarch64 operating system architecture.

Solution

- Upgrade to OpenSSL version 1.1.1e
- Upgrade to OpenSSL version 1.0.2u

Risk factors:
This vulnerability only exists on the x86_64 operating system architecture and does not affect the aarch64 operating system architecture.

Proven Record

Hear From Our Customer

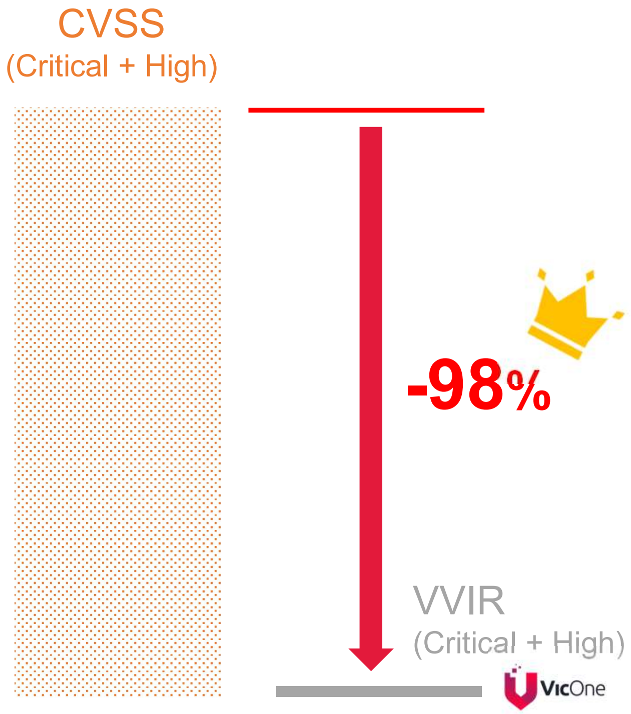
ASKEY

Secure **V2X** with effective vulnerability management

“VicOne helps ASKEY improve product development efficiency ***from six months to two weeks****.”*

YC Chang
Senior Director at Askey’s
Automotive Product Unit

Take ASKEY’s 5G C-V2X OBU as an example:



Source: https://documents.vicone.com/success-story/askey-success-story.pdf

8. Continual cybersecurity activities

8.3 Cybersecurity monitoring

8.4 Cybersecurity event evaluation

8.5 Vulnerability analysis

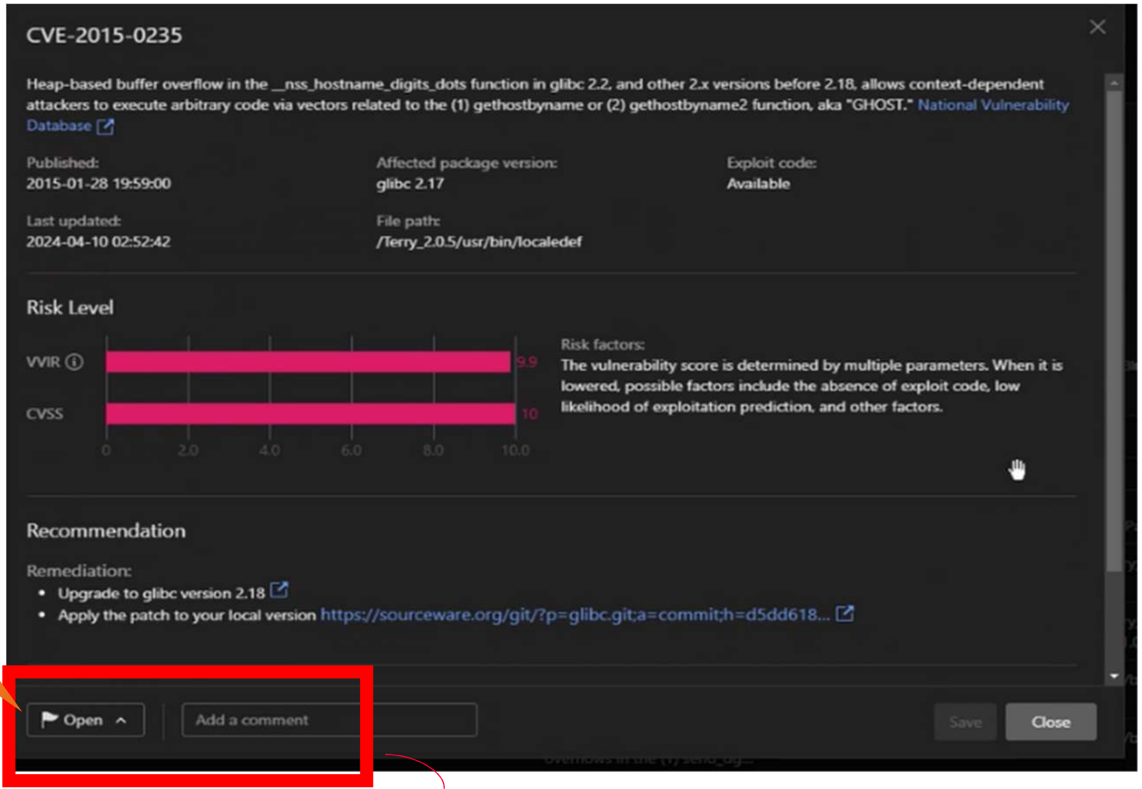
8.6 Vulnerability management

10. Product development

10.4.1 Design

10.4.2 Integration and verification

Integrate with third-party ticketing systems for managing case with ease.



CVE-2015-0235

Heap-based buffer overflow in the __nss_hostname_digits_dots function in glibc 2.2, and other 2.x versions before 2.18, allows context-dependent attackers to execute arbitrary code via vectors related to the (1) gethostbyname or (2) gethostbyname2 function, aka "GHOST." National Vulnerability Database

Published:
2015-01-28 19:59:00

Affected package version:
glibc 2.17

Exploit code:
Available

Last updated:
2024-04-10 02:52:42

File path:
/Terry_2.0.5/usr/bin/localedef

Risk Level

Risk factors:
The vulnerability score is determined by multiple parameters. When it is lowered, possible factors include the absence of exploit code, low likelihood of exploitation prediction, and other factors.

Recommendation

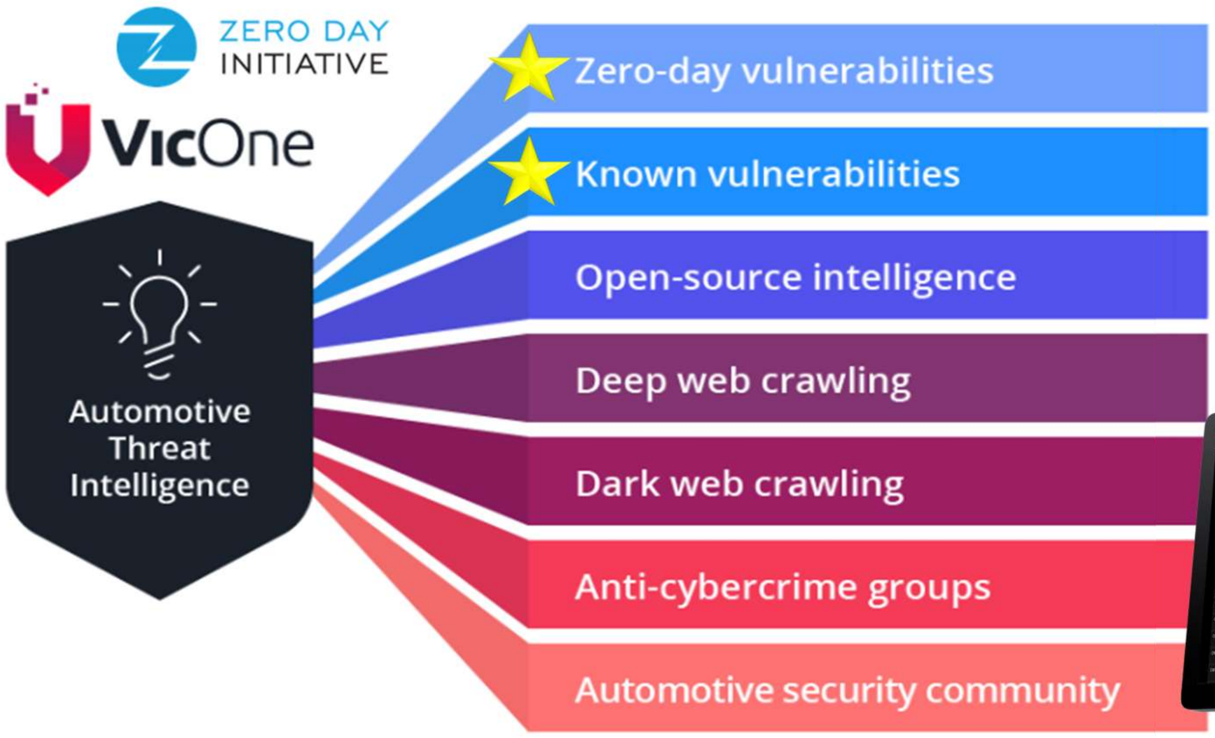
Remediation:

- Upgrade to glibc version 2.18
- Apply the patch to your local version https://sourceware.org/git/?p=glibc.git;a=commit;h=d5dd618...

Open/Close tickets

TICKETING SYSTEM For example: Jira Software

30+ Years of Threat Intelligence



ZERO DAY INITIATIVE

VicOne

Automotive Threat Intelligence

- Zero-day vulnerabilities
- Known vulnerabilities
- Open-source intelligence
- Deep web crawling
- Dark web crawling
- Anti-cybercrime groups
- Automotive security community

Threat Feeds

Vulnerabilities

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

GitHub

AUTOMOTIVE GRADE LINUX

THE LINUX FOUNDATION

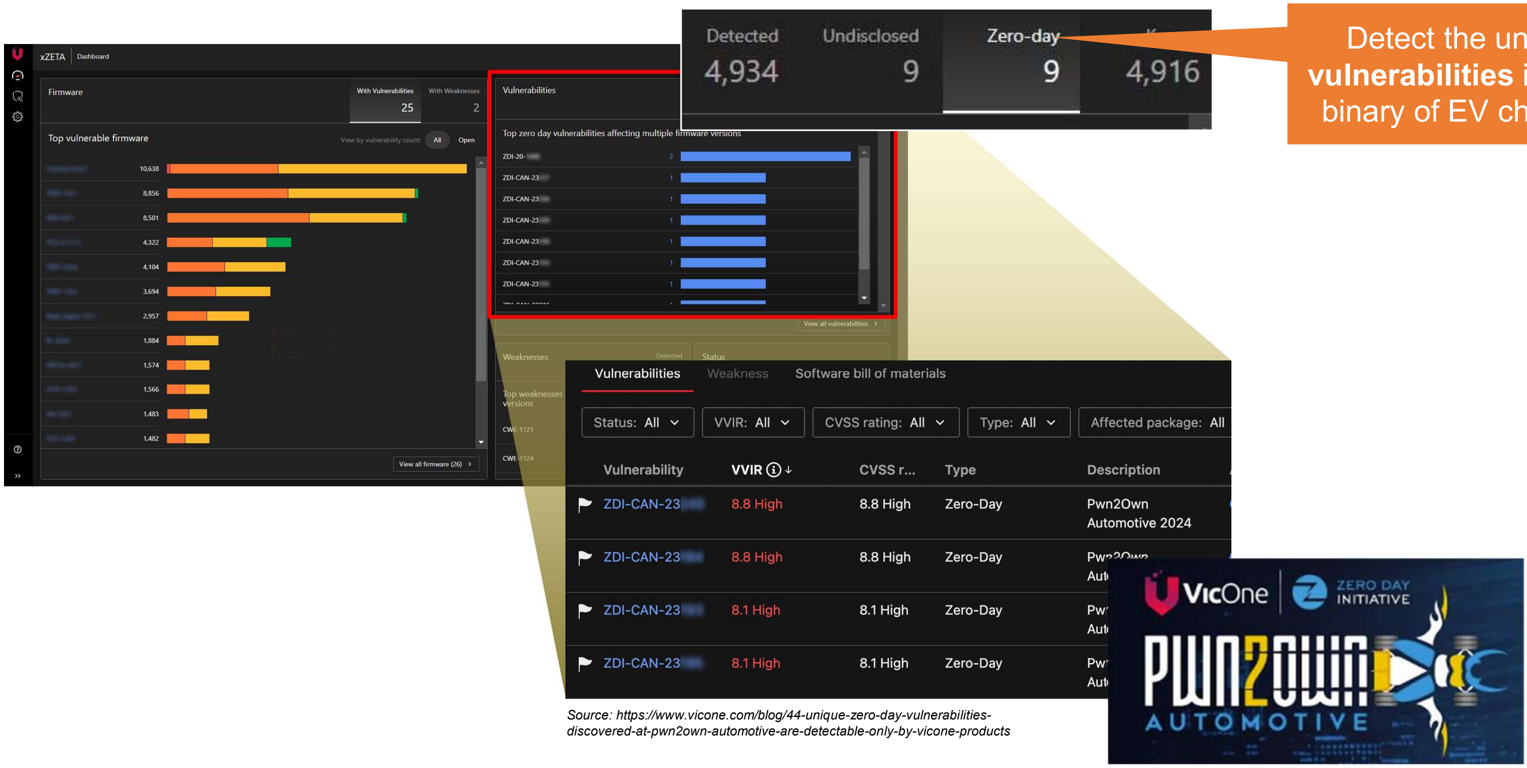
OpenSSF

Exploits, Threat Intel and PoCs

Exploit VEX	Exploit DB	Threat Intel INTEL471
EPSS	Exploit DB	

One and Only:

Detect Zero-Day Vulnerabilities with Unique Automotive Threat Intelligence



ZDI-20-[redacted]	2
ZDI-CAN-23[redacted]	1
ZDI-CAN-23[redacted]	1
ZDI-CAN-23[redacted]	1
ZDI-CAN-23[redacted]	1
ZDI-CAN-23[redacted]	1
ZDI-CAN-23[redacted]	1

Detected	Undisclosed	Zero-day
4,934	9	9

4,916

Status: All | VVIR: All | CVSS rating: All | Type: All | Affected package: All

Vulnerability	VVIR ⓘ ↓	CVSS r...	Type	Description
ZDI-CAN-23[redacted]	8.8 High	8.8 High	Zero-Day	Pwn2Own Automotive 2024
ZDI-CAN-23[redacted]	8.8 High	8.8 High	Zero-Day	Pwn2Own Aut
ZDI-CAN-23[redacted]	8.1 High	8.1 High	Zero-Day	Pw Aut
ZDI-CAN-23[redacted]	8.1 High	8.1 High	Zero-Day	Pw Aut

Detect the unique **zero-day vulnerabilities** in the firmware or binary of EV charging systems.

Source: https://www.vicone.com/blog/44-unique-zero-day-vulnerabilities-discovered-at-pwn2own-automotive-are-detectable-only-by-vicone-products

Benefits

Accelerating ISO/SAE 21434 Vulnerability Management

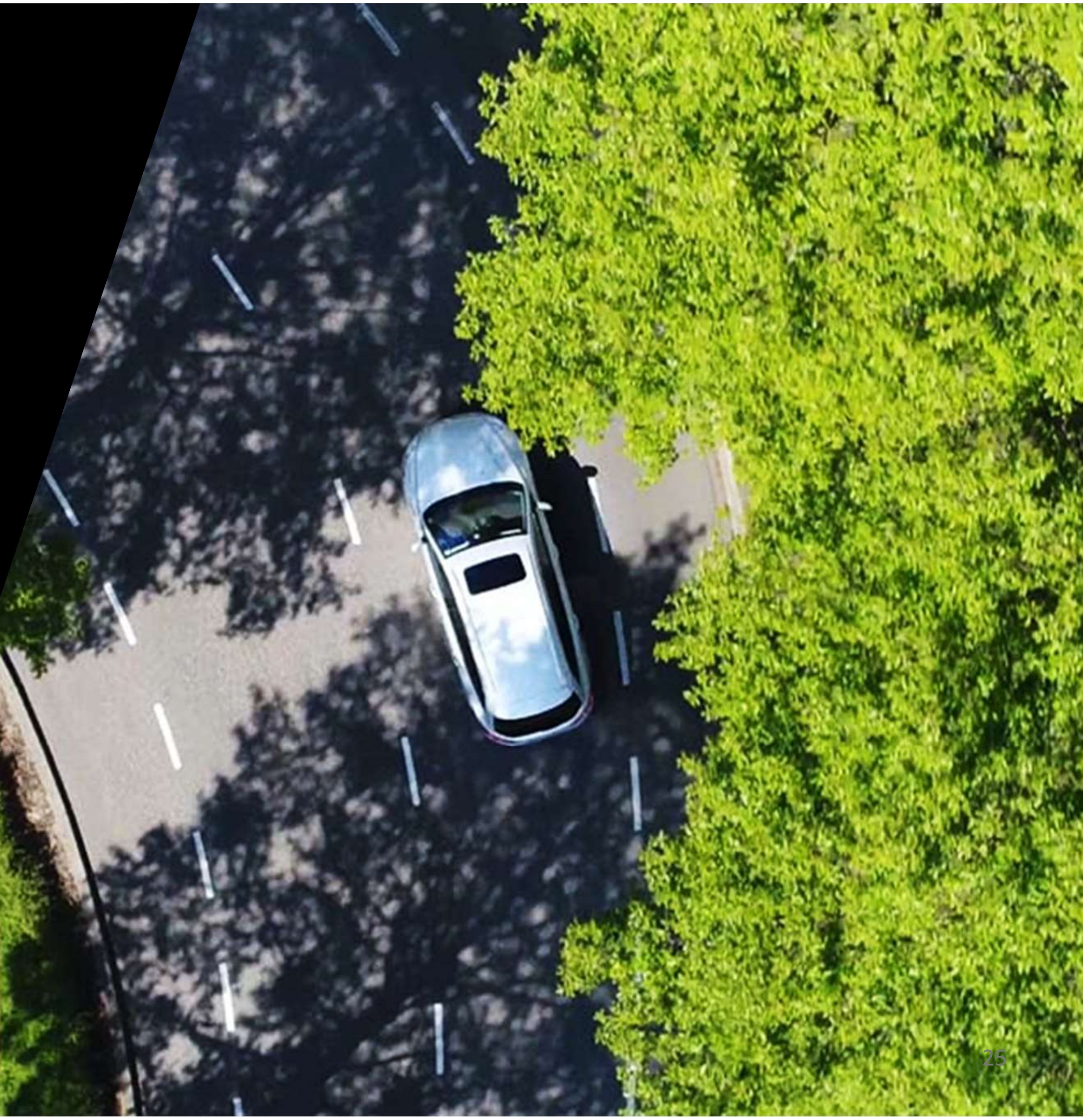
Reduce software risk mitigation from 6 months to 2 weeks. **Save around €14K*.**

The Best Coverage

Eliminate blind spots with 27% more coverage, including unique zero-day threat intelligence

> We utilize the xZETA system to demonstrate our effective vulnerability management capabilities to auditors, which **helps us meet the requirements of UN R155.**

TIN T. NGUYEN
Director
Automotive Cybersecurity Division, VinCSS



VicOne

Driving Automotive Cybersecurity Forward