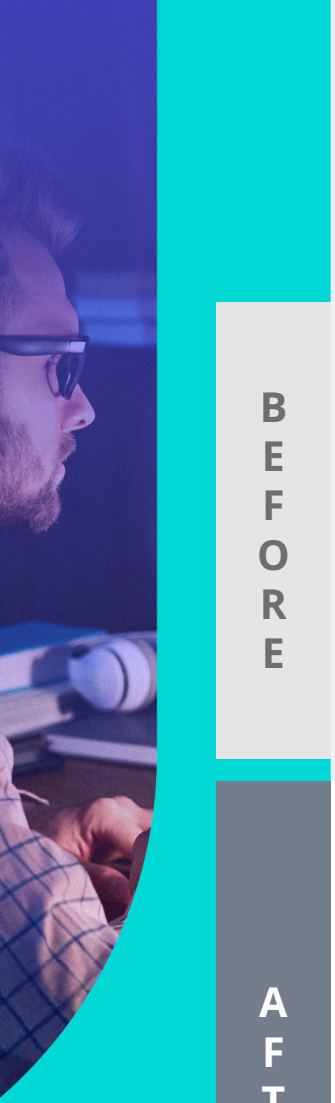
VicOne

USE CASE

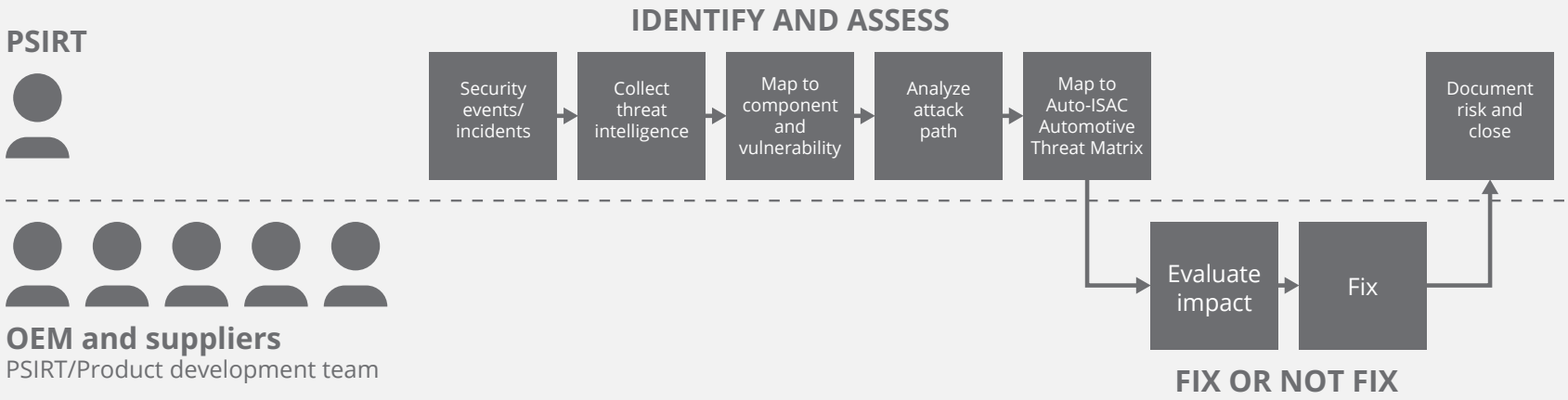
From Hours to Seconds

Simplify Your Attack Path Analysis With xZETA

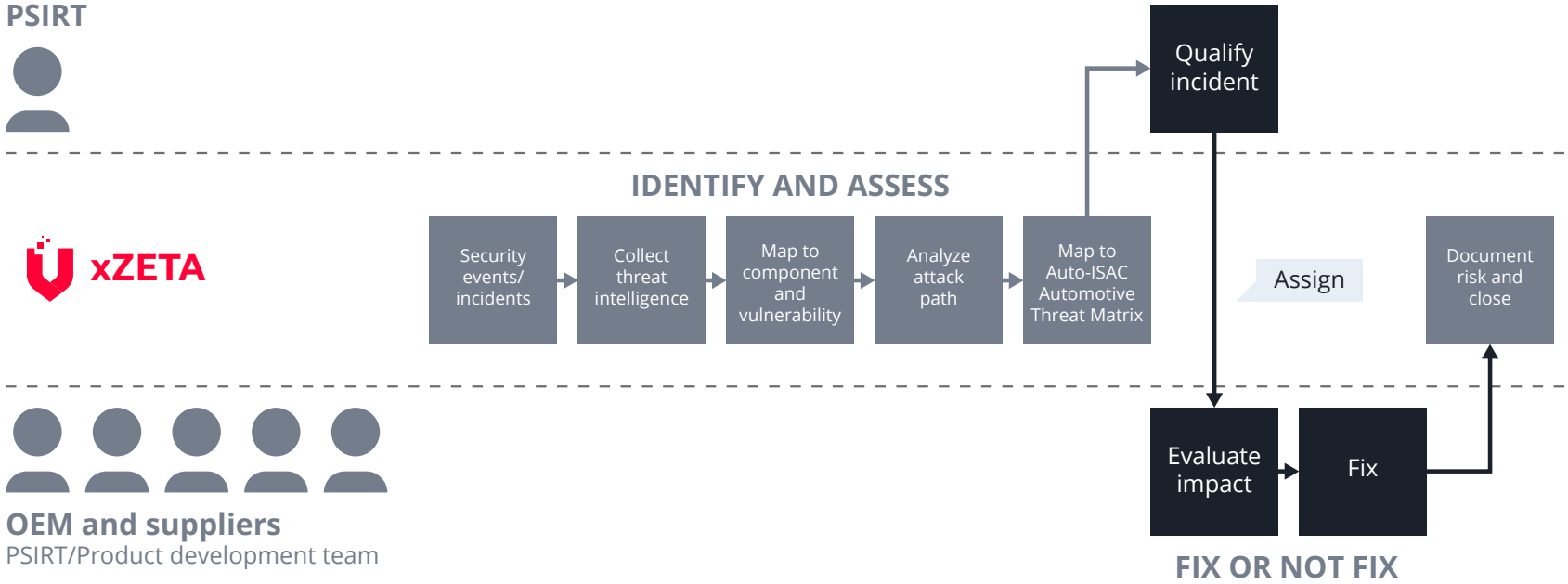


How xZETA Enables the PSIRT to Focus on Incident Response — the Most Critical Task

BEFORE



AFTER



USE CASE

Zero-Click Exploit Targeting MCUs: Taking Control of the IVI via Wi-Fi

[redacted]'s Zero-click Vulnerabilities Allowed its Car to be Hacked Remotely Using Drones

The zero-click vulnerabilities, which the researchers named "TBONE," were originally scheduled to be showcased at [redacted]'s "Pwn2Own 2020" hacking event.

CVE-2021-3347 Detail

MODIFIED

This vulnerability has been modified since it was last analyzed by the NVD. It is awaiting reanalysis which may result in further changes to the information provided.

Description

An issue was discovered in the Linux kernel through 5.10.11. PI futexes have a kernel stack use-after-free during fault handling, allowing local users to execute code in the kernel, aka CID-34b1a1ce1458.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

NIST: NVD **Base Score:** 7.8 HIGH **Vector:** CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

AFTER

PSIRT

xZETA

1 ISO/SAE 21434 8.3 “Cybersecurity monitoring”

IDENTIFY AND ASSESS

Security events/ incidents → Collect threat intelligence → Map to component and vulnerability → Analyze attack path → Map to Auto-ISAC Automotive Threat Matrix

Qualify incident

Assign

Document risk and close

Evaluate impact → Fix

FIX OR NOT FIX

OEM and suppliers

PSIRT / product development team

Incident detai | Related vulnerabilities

Maps the incident’s attack path with relevant exploited vulnerabilities

Summary

Attack type: ZDI
Approach: Short-Range Wireless Communication
Affected vendor: [redacted]
Target: Wi-Fi, IVI System
Impact: Vehicle

- In vehicle (1): IVI System

Description 2024-06-11 | Source

Researchers Ralf-Philipp and Benedikt Schmotzle discovered a remote zero-click security vulnerability in an open-source component in [redacted] automobiles. Hackers who use this vulnerability can gain control over the car’s infotainment system remotely over Wi-Fi. Thankfully, this attack will not allow hackers drive control.

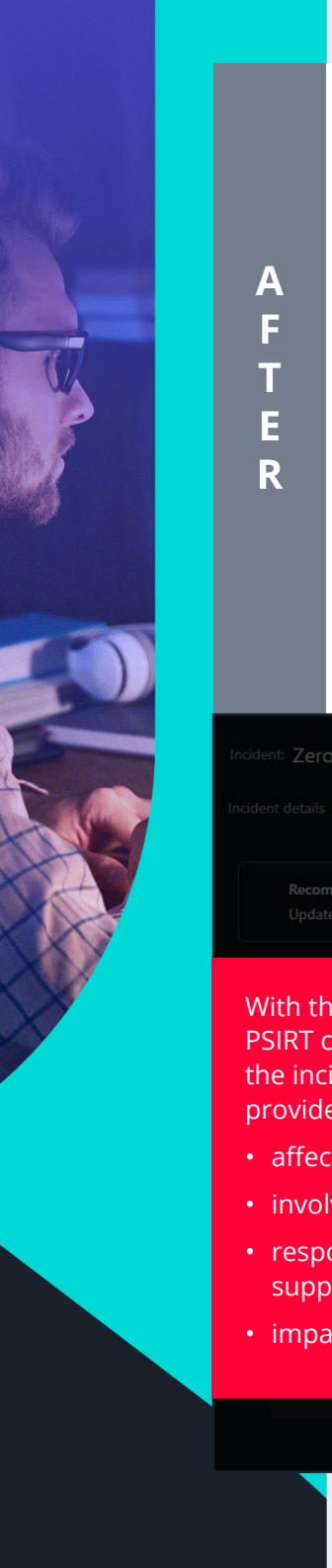
Attack Phase Overview

Manipulate Environment → Persistence → Lateral Movement → Affect Vehicle Function → Impact

Attack path with TTPs

View UN R155 Reference

	Activity	Technique ID	Attack phase
1	Initial entry over Wi-Fi.	T1465 - Rogue Wi-Fi Access Points	Manipulate Environment
2	Exploit DHCP stack.	T1210 - Exploitation of Remote Services	Lateral Movement
3	Privilege escalation on the MCU.	T1404 - Exploitation for Privilege Escalation	Persistence
			Persistence



AFTER

PSIRT

2

Qualify incident

IDENTIFY AND ASSESS

xZETA

Security events/ incidents → Collect threat intelligence → Map to component and vulnerability → Analyze attack path → Map to Auto-ISAC Automotive Threat Matrix

Assign

Document risk and close

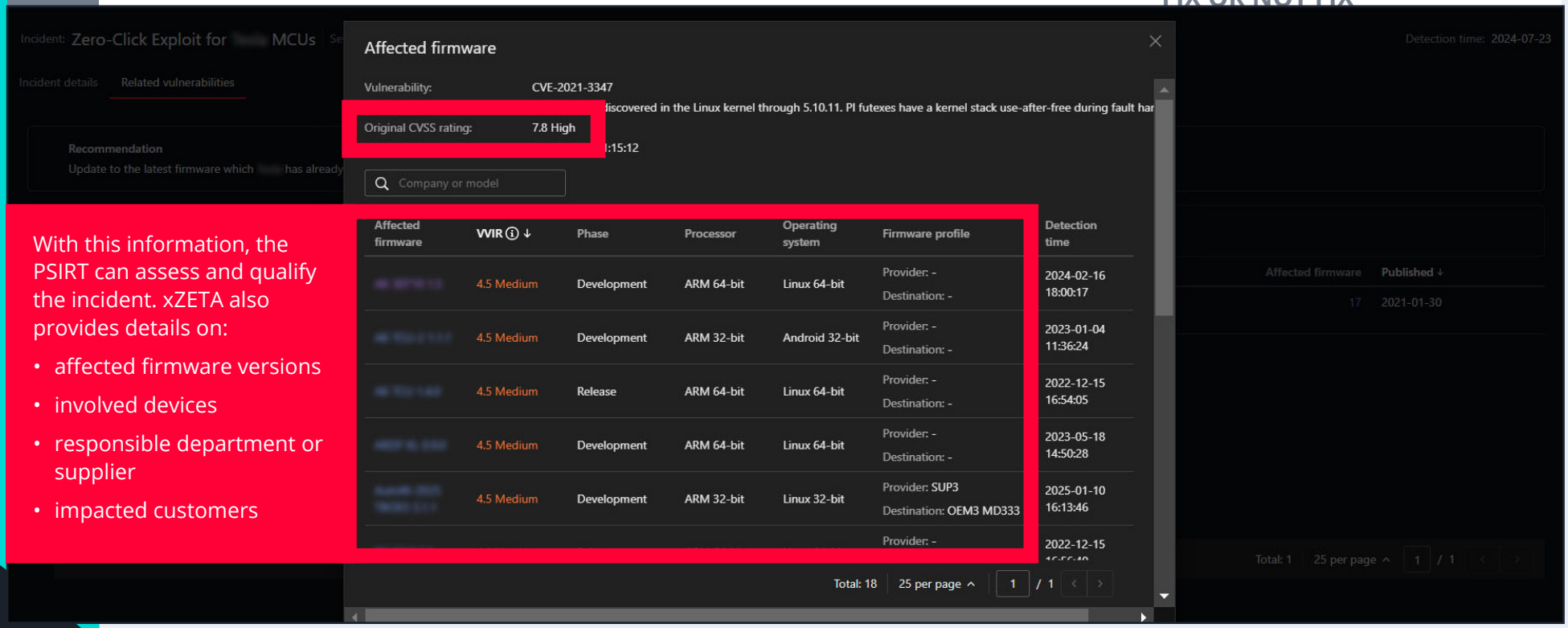
Evaluate impact → Fix

FIX OR NOT FIX

OEM and suppliers

PSIRT / product development team

ISO/SAE 21434
8.4 “Cybersecurity event evaluation”
8.5 “Vulnerability analysis”



With this information, the PSIRT can assess and qualify the incident. xZETA also provides details on:

- affected firmware versions
- involved devices
- responsible department or supplier
- impacted customers

AFTER

PSIRT

xZETA

IDENTIFY AND ASSESS

Security events/ incidents → Collect threat intelligence → Map to component and vulnerability → Analyze attack path → Map to Auto-ISAC Automotive Threat Matrix → Qualify incident

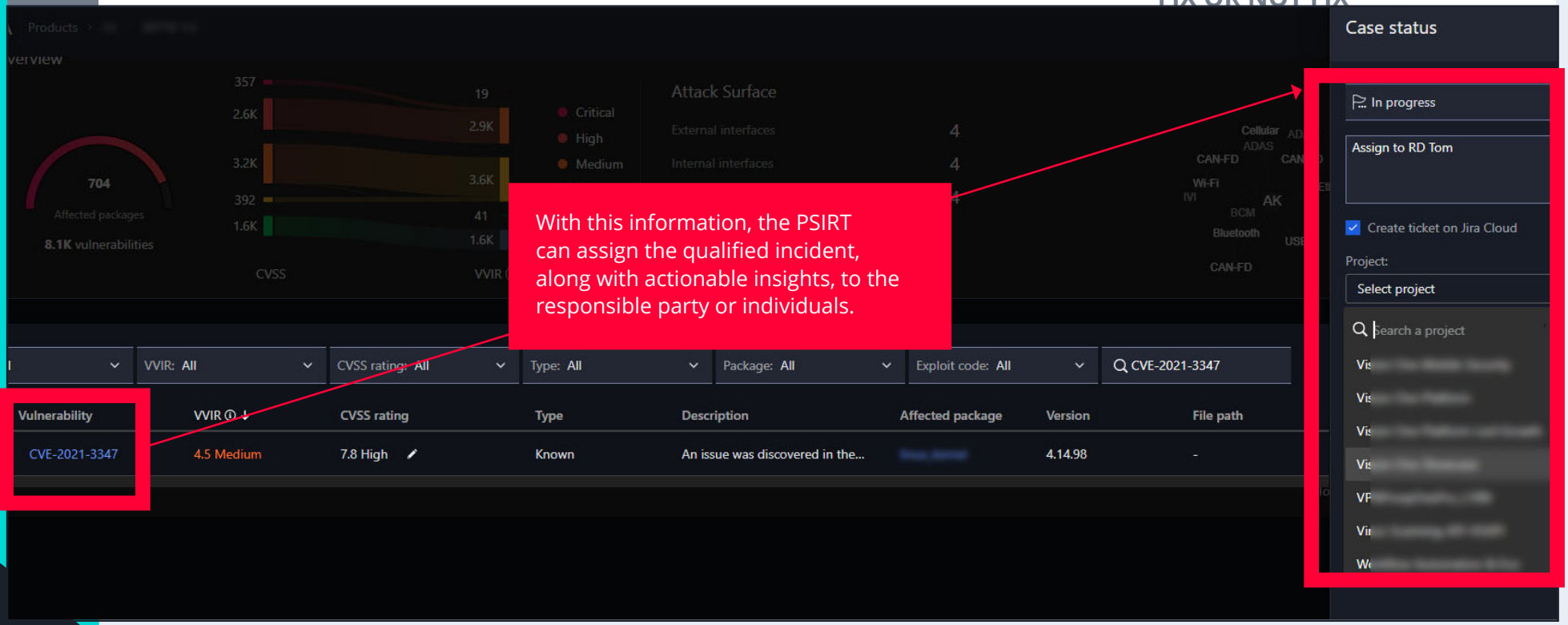
Qualify incident → Assign (3) → Document risk and close

Assign (3) → Evaluate impact → Fix

FIX OR NOT FIX

OEM and suppliers
PSIRT / product development team

ISO/SAE 21434
8.4 "Cybersecurity event evaluation"
8.5 "Vulnerability analysis"



With this information, the PSIRT can assign the qualified incident, along with actionable insights, to the responsible party or individuals.

AFTER

PSIRT

xZETA

OEM and suppliers
PSIRT / product development team

IDENTIFY AND ASSESS

Security events/ incidents → Collect threat intelligence → Map to component and vulnerability → Analyze attack path → Map to Auto-ISAC Automotive Threat Matrix → Qualify incident

ISO/SAE 21434
8.6 "Vulnerability management"

4

Assign

Document risk and close

Evaluate impact → Fix

FIX OR NOT FIX

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

	Vulnerability	VVIR	CVSS rating	Type	Description	Affected package	Version	File path	Expl cod
☐	CVE-2014-6271	9.8 Critical	9.8 Critical	Known	GNU Bash through 4.3 process...	bash	4.2.46	/usr/bin/bash	✓
✓	Closed 021-3347				issue was discovered in the...	linux_kernel	4.14.98	-	-
☐	CVE-2018-5740	7.9 High	7.5 High	Known	"deny-answer-aliases" is a littl...	bind-license	9.11.4	/usr/share/licenses/bind-licens...	-
☐	CVE-2020-8617	7.5 High	5.9 Medium	Known	Using a specially-crafted mess...	bind-license	9.11.4	/usr/share/licenses/bind-licens...	✓
☐	CVE-2020-8625	7.2 High	8.1 High	Known	BIND servers are vulnerable if ...	bind-license	9.11.4	/usr/share/licenses/bind-licens...	-
☐	CVE-2021-25216	6.7 Medium	9.8 Critical	Known	In BIND 9.5.0 -> 9.11.29, 9.12....	bind-license	9.11.4	/usr/share/licenses/bind-licens...	-

Once the incident is resolved, a note is added to the system to close the case.

xZETA

Superior Automotive Vulnerability and SBOM Management System

Gather

- Binaries/ Firmware
- Third-party SBOM
- Third-party HBOM
- Open-source/ Third-party application

xZETA

Achieve With Ease

- XBOM management
- Vulnerability management
- APT/Ransomware detection
- Private vulnerability database creation
- Sensitive data leak detection
- License compliance

Gain Instant Access to Automotive **Threat Intelligence**

xZETA offers automotive threat intelligence, tracking global cybersecurity incidents and correlating them with vulnerabilities. This helps OEMs and suppliers understand exploitation methods and **map attack paths with context**.

Get the Best Coverage With **189% More**

xZETA provides 189% more coverage than the National Vulnerability Database (NVD), including **zero-day vulnerabilities, undisclosed risks, customer-discovered vulnerabilities**, and more.

Enhance Operational **Efficiency**

xZETA streamlines the ISO/SAE 21434 workflow with seamless **TARA tool integration** and smooth connectivity to **third-party ticketing systems** for efficient case management.

VicOne

Reduce Attack Path Analysis Time From Hours to Seconds

Enabling Faster Response and Mitigation With xZETA

REQUEST A DEMO

xZETA

Learn more about VicOne by visiting VicOne.com or scanning this QR code: