Intrusion Detection Use Case and Secure Components

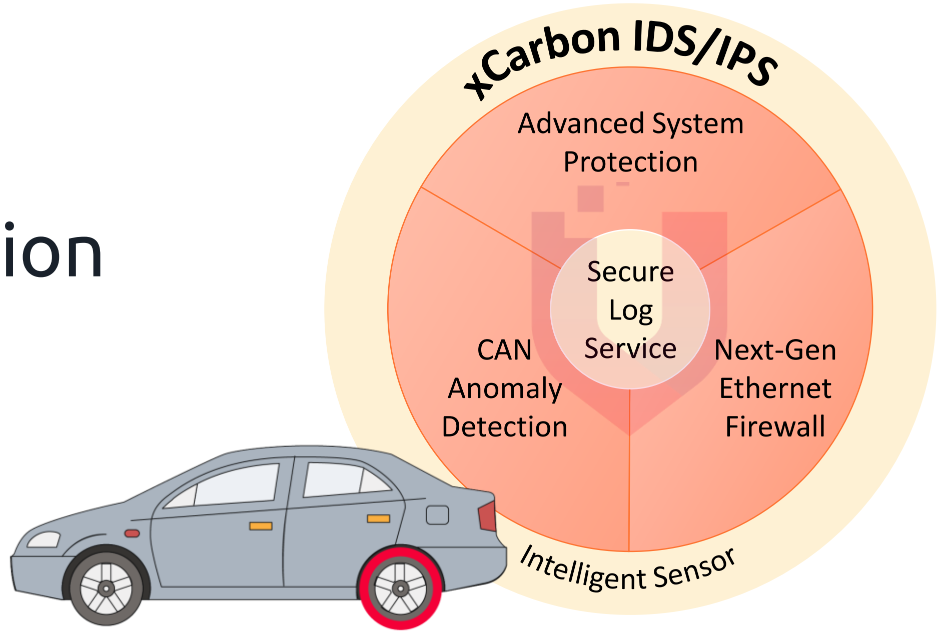
Protect your on-board ECUs from threats with a frictionless intrusion detection and prevention system (IDS/IPS)

Kalli Schlauch - CEH, GCIH

VicOne

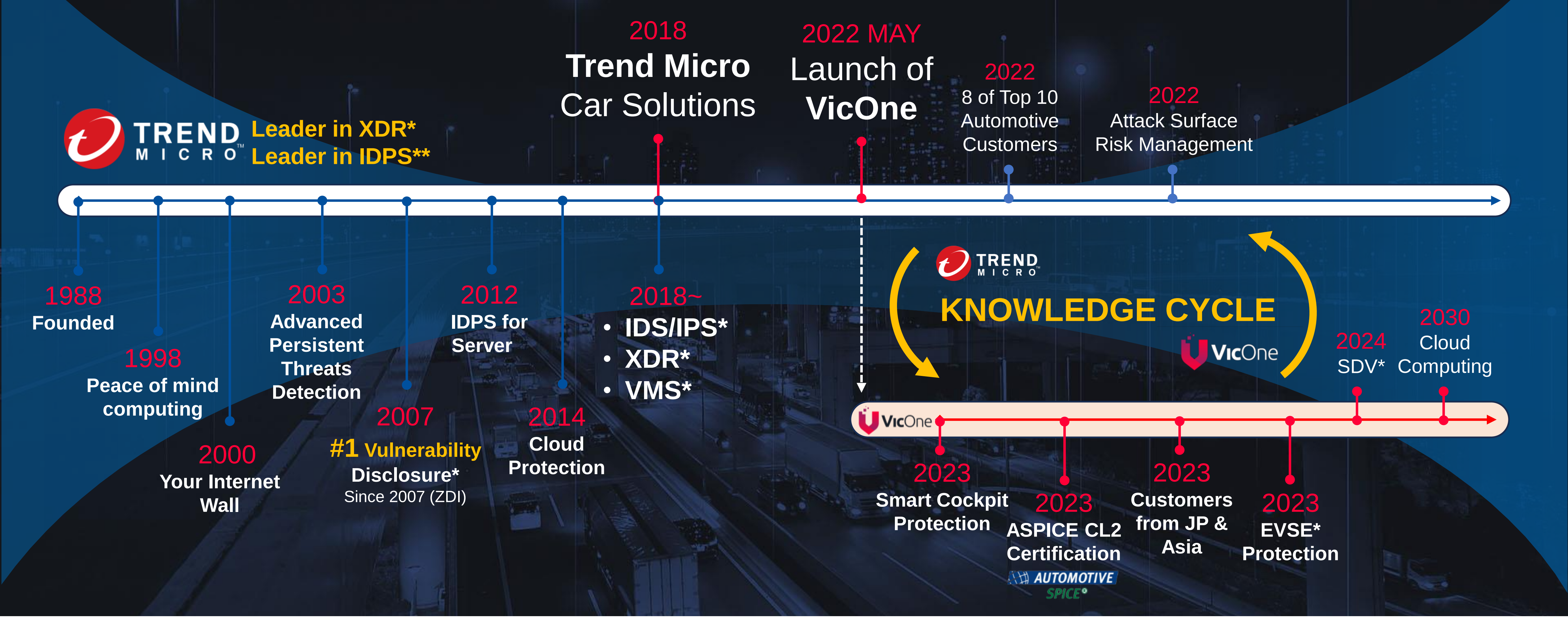
Agenda

1. About VicOne
2. Emerging Security Risks in Software-Defined Vehicles
3. Expanding Threat Landscape
4. Intrusion Detection and Prevention



About VicOne

From Trend to **VicOne**: Always Anticipating, Adapting



Leader in XDR*
Leader in IDPS**

1988
Founded

1998
Peace of mind computing

2000
Your Internet Wall

2003
Advanced Persistent Threats Detection

2007
#1 Vulnerability Disclosure*
Since 2007 (ZDI)

2012
IDPS for Server

2014
Cloud Protection

2018
Trend Micro
Car Solutions

2018~
- IDS/IPS*
- XDR*
- VMS*

2022 MAY
Launch of
VicOne

2022
8 of Top 10 Automotive Customers

2022
Attack Surface Risk Management

KNOWLEDGE CYCLE

2023
Smart Cockpit Protection

2023
ASPICE CL2 Certification

2023
Customers from JP & Asia

2023
EVSE* Protection

2024
SDV*

2030
Cloud Computing

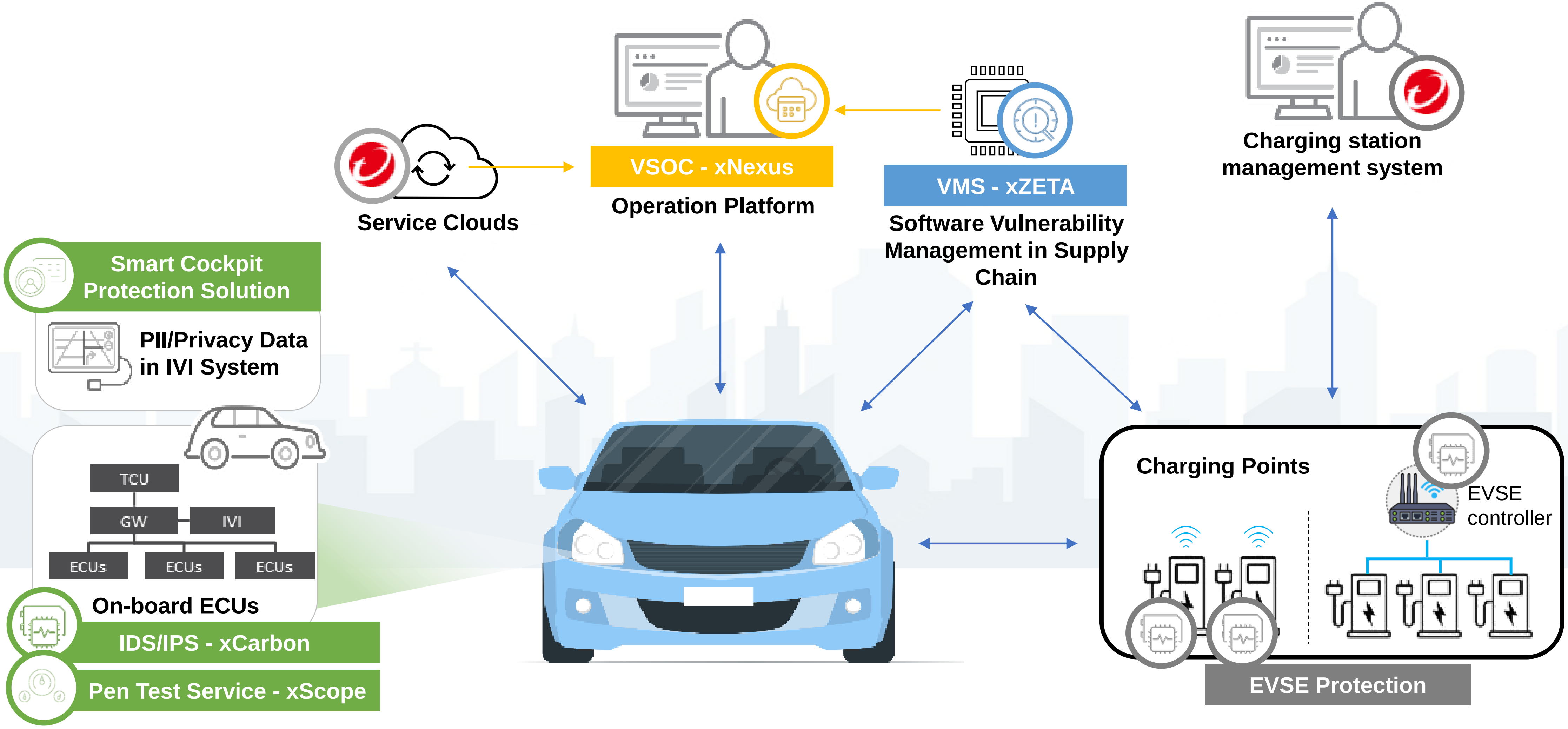
1. Forrester Wave, Extended Detection and Response (XDR), Q4, 2021
2. Gartner, Enterprise Network Equipment by Market Segment, Worldwide, 2021.
3. Quantifying the Public Vulnerability Market, Omdia, May 2022

- IDS/IPS = Intrusion Detection and Prevention System
- XDR = Extended detection and response
- VMS = Vulnerability management system

- EVSE = Electric Vehicle Supply Equipment
- SDV = Software-defined vehicle

Comprehensive Cybersecurity Solutions for CASE Vehicles/SDVs

- For Head of SW Development
- For Head of Cybersecurity Operations
- For Head of Digital Service
- For Head of Vehicle Cybersecurity
- For Head of EVSE Cybersecurity



Service Clouds

VSOC - xNexus

Operation Platform

VMS - xZETA

Software Vulnerability Management in Supply Chain

Charging station management system

Smart Cockpit Protection Solution

PII/Privacy Data in IVI System

On-board ECUs

IDS/IPS - xCarbon

Pen Test Service - xScope

Charging Points

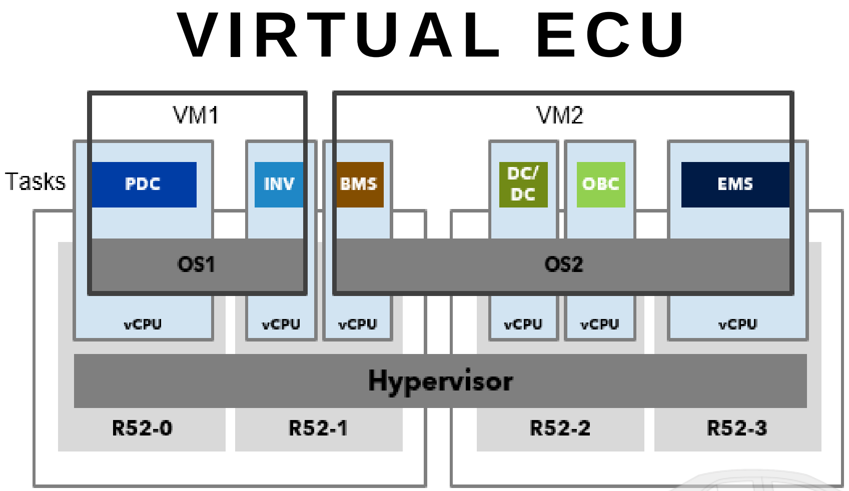
EVSE controller

EVSE Protection

Emerging Security Risks in Software-Defined Vehicles

Expanding Threat Landscape

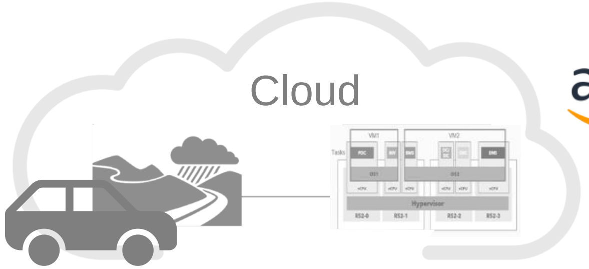
Virtual ECU Advancements fuel SDV



NXP Qualcomm

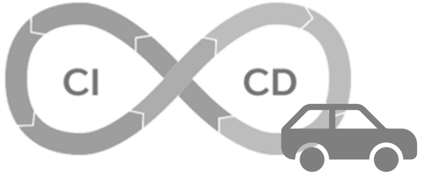
Picture Credit: NXP

Feasibility of Digital Twin for system integration simulation



aws SOAFEE

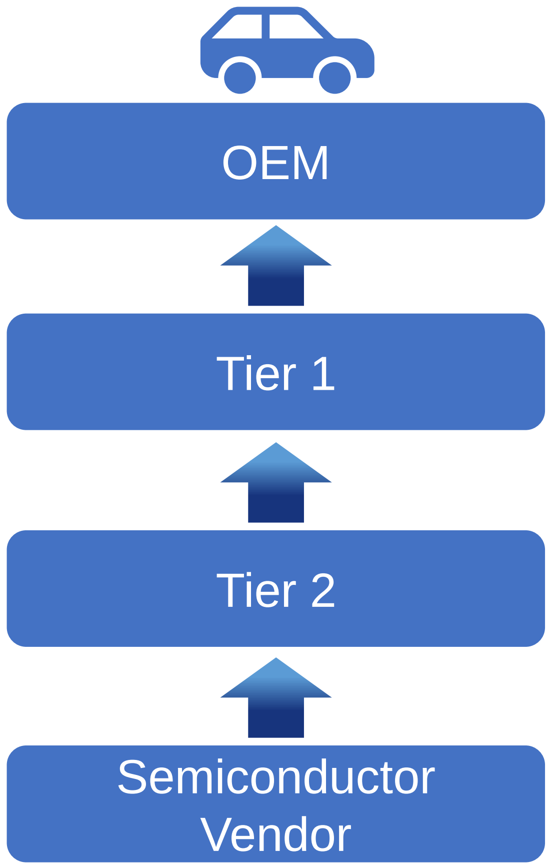
Implementing CI/CD for accelerated vehicle design process



Realizing Updateable Local Systems for advanced software integration

Automotive Ecosystem Evolved

TIERED



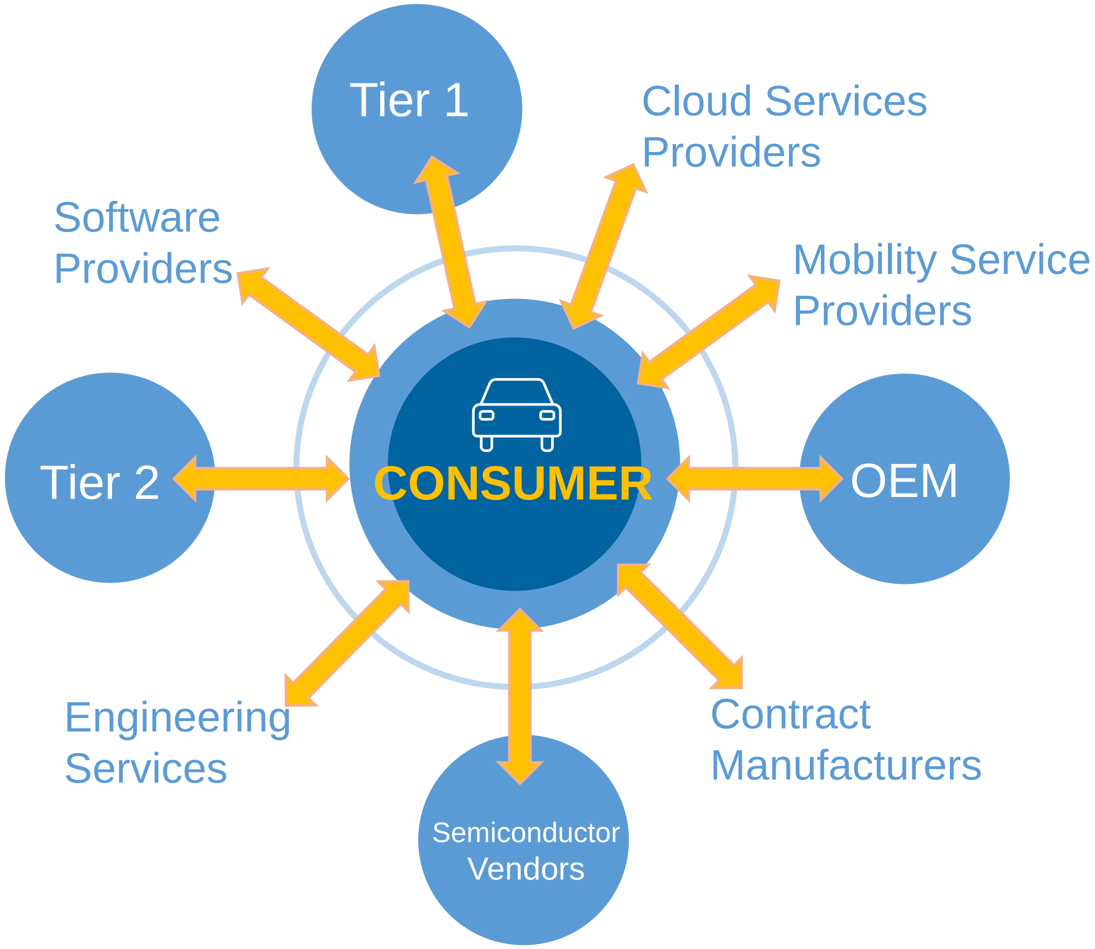
OEM

Tier 1

Tier 2

Semiconductor Vendor

BIDIRECTIONAL & INTERCONNECTED



Tier 1

Cloud Services Providers

Software Providers

Mobility Service Providers

Tier 2

CONSUMER

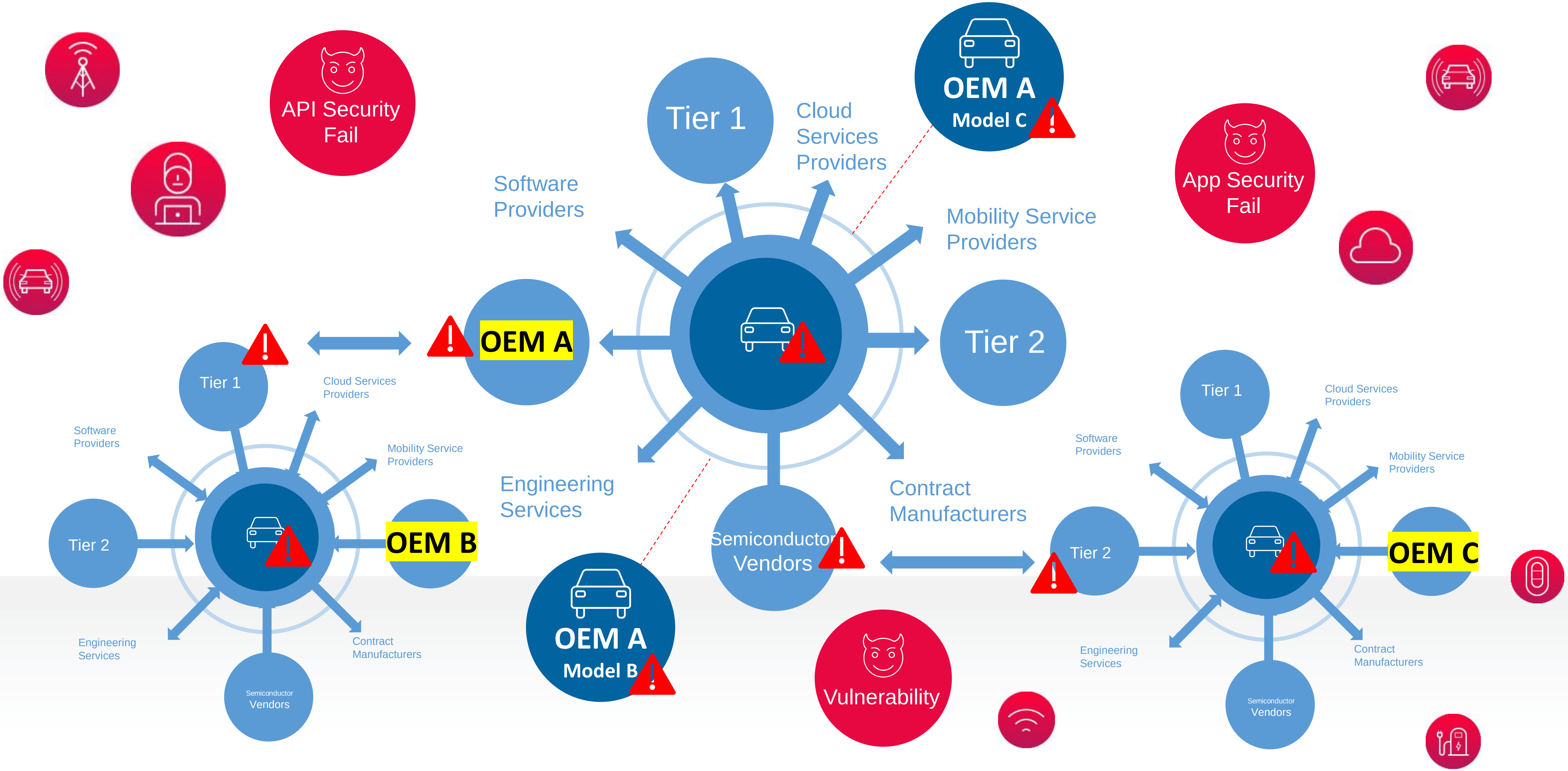
OEM

Engineering Services

Contract Manufacturers

Semiconductor Vendors

Threat landscape – Wider and more open



Risks in SDV

👍

😈

Development Lifecycle

Speed Up Innovation with Open and Standardize

- **Open-source software vulnerabilities** in the entire automotive ecosystem

Cloud Services

Updatable User Experience with Cloud-Car Connected

- Connected **ecosystem vulnerability** from V2X
- Cloud to edge/edge to cloud
- **Frequent OTA** updates
- Higher usage of API

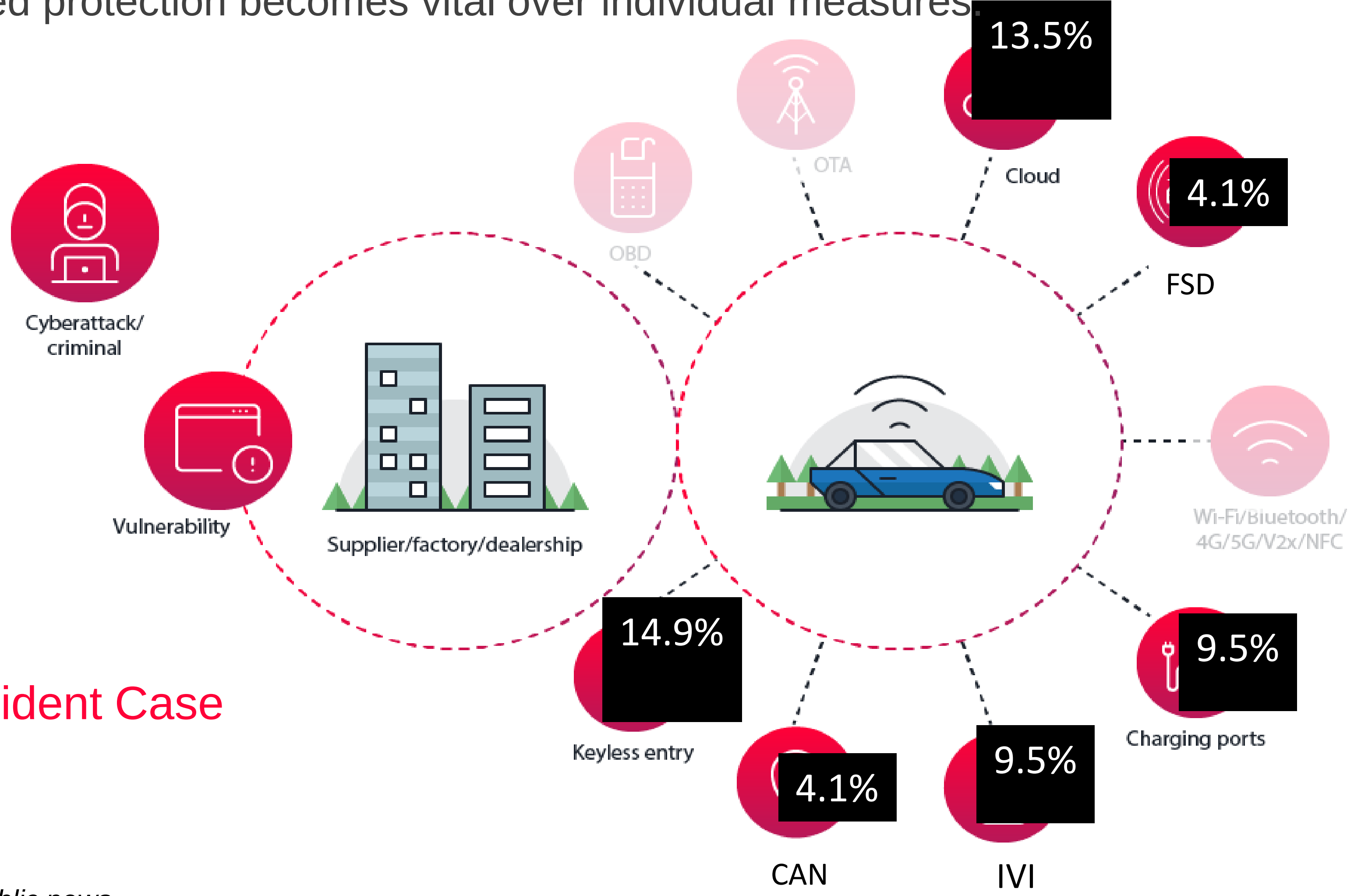
Physical Car

Simplified Development with Centralized HPC

- Widespread adoption of **virtualization** technologies
- In-vehicle **network security** risks
- **Privacy concerns** surrounding user profiles

Expanding Attack Landscape

- 2023 H1 incident cases show a **broader spectrum** of attacks targeting vehicles, expanding from the cloud to encompass components and infrastructure.
- Showing integrated protection becomes vital over individual measures.

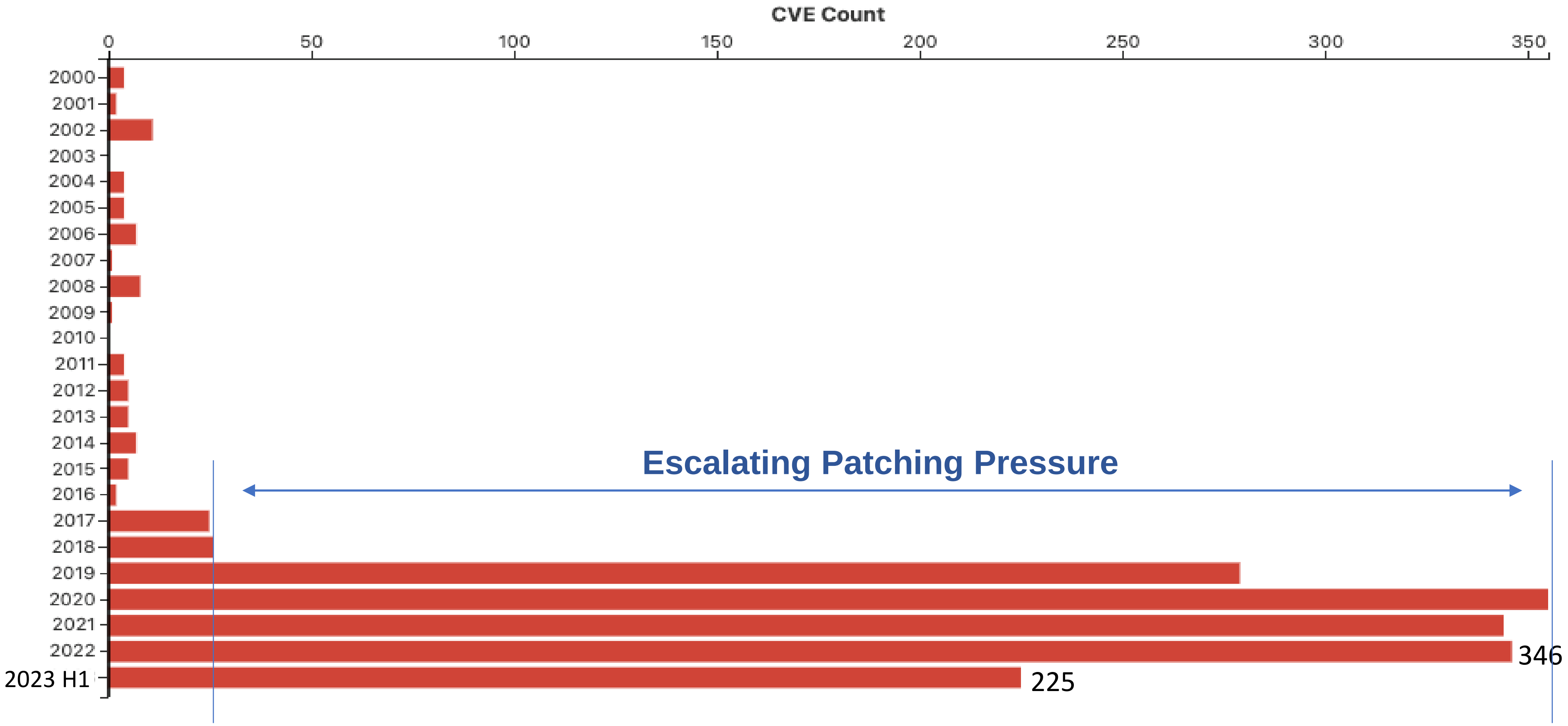


2023 H1 Incident Case
(by category)

Source: VicOne and public news

30% CVEs YoY Increased

- 2023 H1 automotive-related CVEs show a **30% YoY increase** from last year.
- Since 2019, there has been an average of **300** automotive-related CVEs per year.
- The continuous rise in CVEs highlight the importance of effective vulnerability management.



Escalating Patching Pressure

Source: VicOne and NVD database

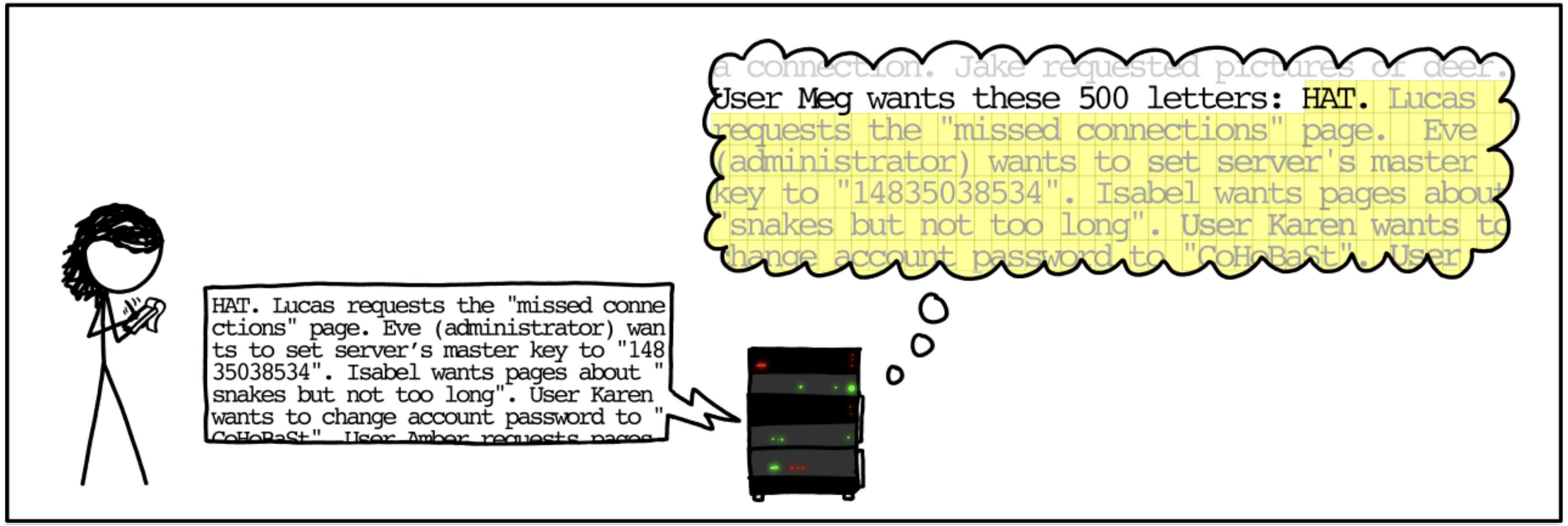
Effects of Exposed Vulnerabilities in Automotive Systems, for example: Data theft/harvest, Device hijack, Device malfunction, Loss of system/service availability, Network host services disabled….

Intrusion Detection and Prevention

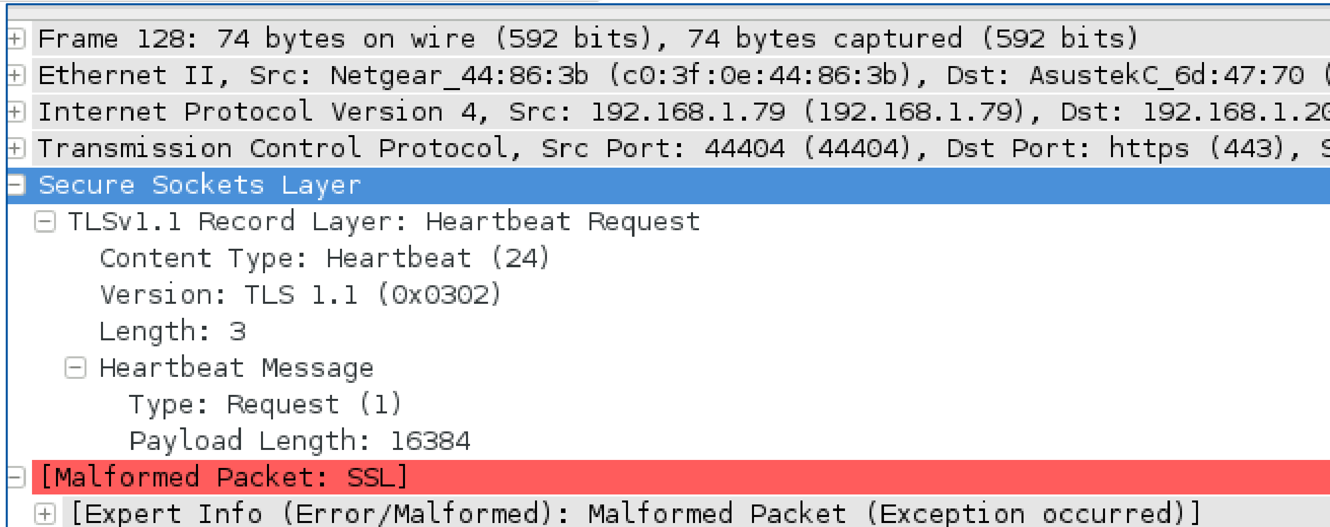
Vulnerability in detail

OpenSSL Heart Bleed

Ironically OpenSSL is Security Library (Secure Sockets Layer Protocol)


a connection. Jake requested pictures of deer. User Meg wants these 500 letters: HAT. Lucas requests the "missed connections" page. Eve (administrator) wants to set server's master key to "14835038534". Isabel wants pages about "snakes but not too long". User Karen wants to change account password to "CoHoBaSt". User
HAT. Lucas requests the "missed conne ctions" page. Eve (administrator) wan ts to set server's master key to "148 35038534". Isabel wants pages about " snakes but not too long". User Karen wants to change account password to " CoHoBaSt". User Amber requests pages

How do we get our hands on those?



```
⊞ Frame 128: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⊞ Ethernet II, Src: Netgear_44:86:3b (c0:3f:0e:44:86:3b), Dst: AsustekC_6d:47:70 (
⊞ Internet Protocol Version 4, Src: 192.168.1.79 (192.168.1.79), Dst: 192.168.1.20
⊞ Transmission Control Protocol, Src Port: 44404 (44404), Dst Port: https (443), S
⊟ Secure Sockets Layer
  ⊟ TLSv1.1 Record Layer: Heartbeat Request
      Content Type: Heartbeat (24)
      Version: TLS 1.1 (0x0302)
      Length: 3
    ⊟ Heartbeat Message
        Type: Request (1)
        Payload Length: 16384
⊟ [Malformed Packet: SSL]
  ⊞ [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
```

- https://xkcd.com/1354/
- https://stackoverflow.com

The Real Case of Tesla Cars

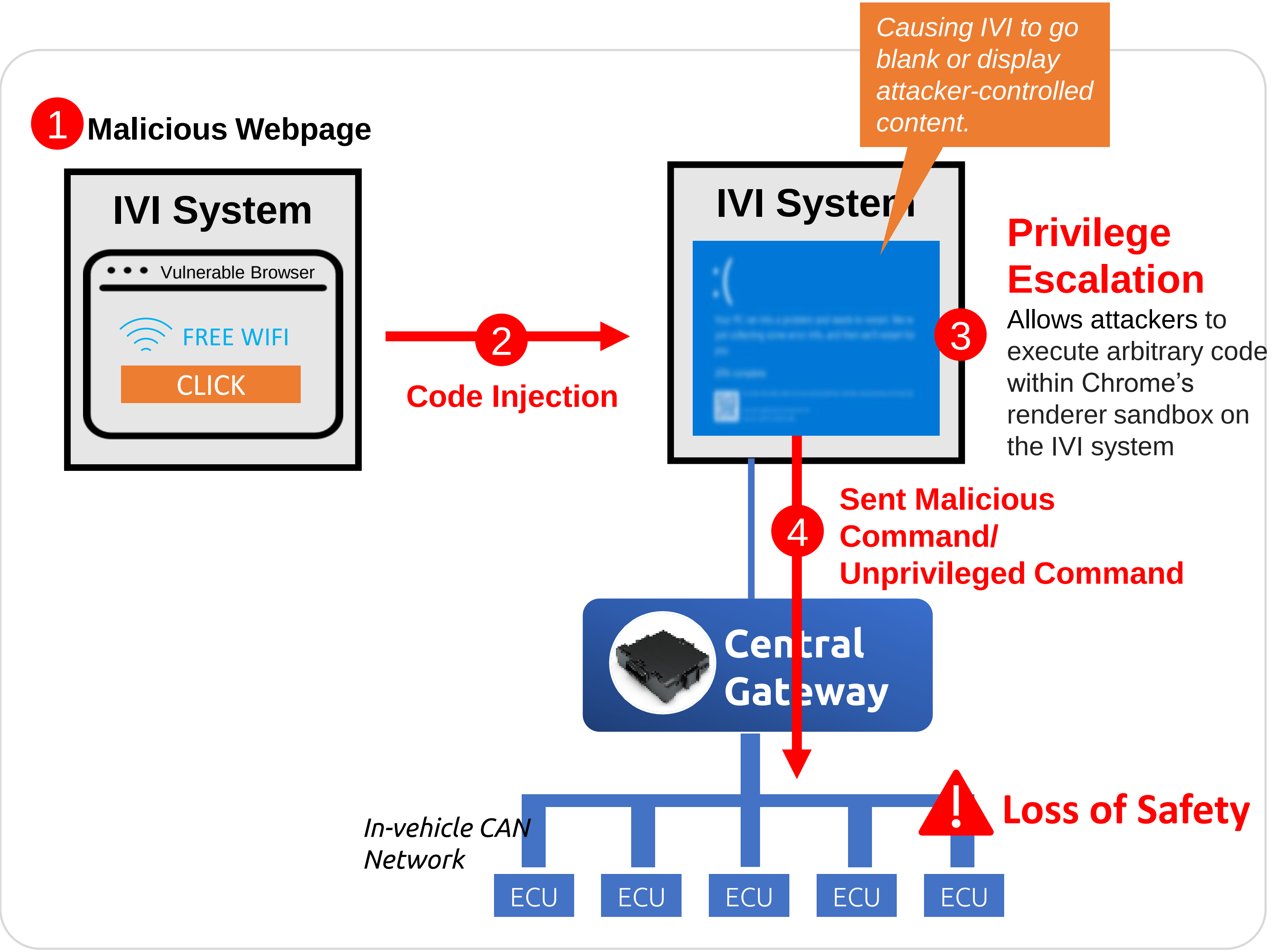
Experimental security assessment in 2019

Hackers conquer Tesla's in-car web browser

Source: ZDI (2019)

Zero Day Initiative @thezdi · Follow

That's a wrap! Congrats to @fluoroacetate on winning Master of Pwn. There total was $375,000 (plus a vehicle) for the week. Superb work from this great duo.



Causing IVI to go blank or display attacker-controlled content.

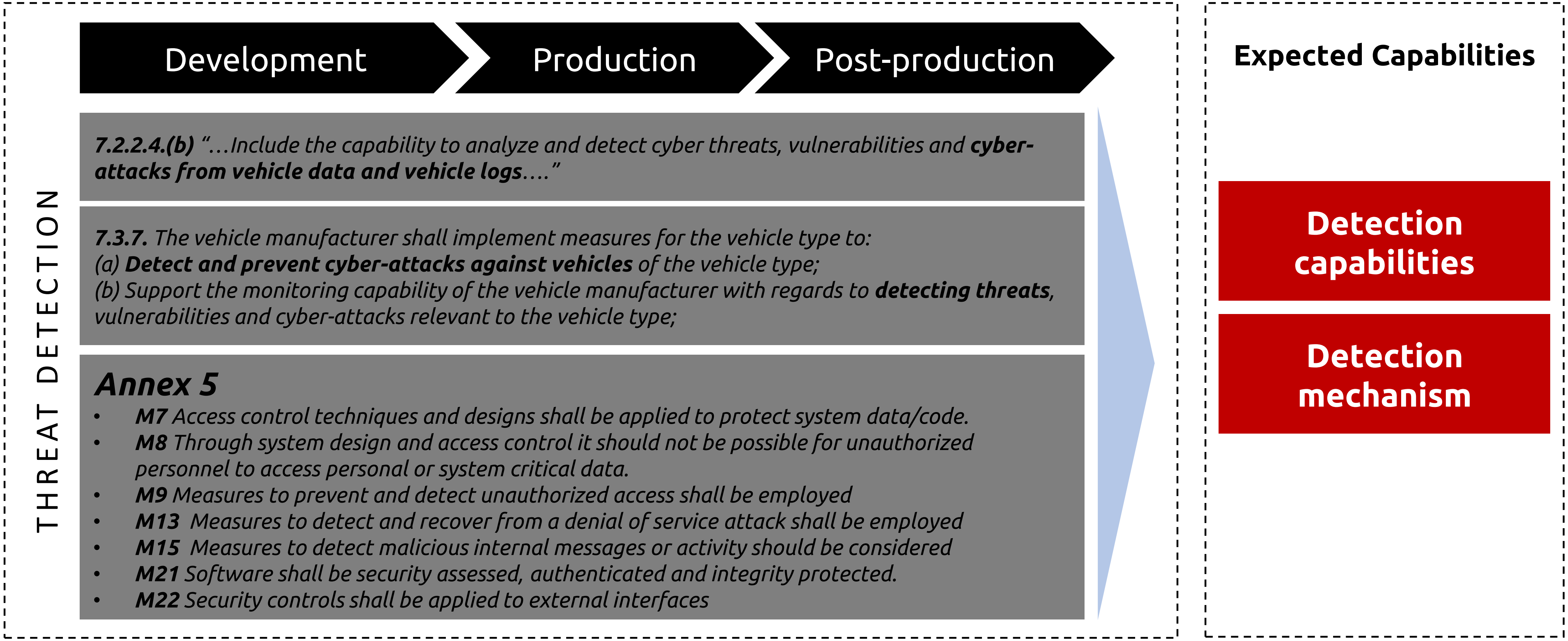
Privilege Escalation

Allows attackers to execute arbitrary code within Chrome's renderer sandbox on the IVI system

UN R155 requires **competent detection capabilities**

Though not mentioned directly in the regulation, IDS becomes an inherent component of vehicle security.

UNECE



7.2.2.4.(b) *"…Include the capability to analyze and detect cyber threats, vulnerabilities and* ***cyber-attacks from vehicle data and vehicle logs****…."*

7.3.7. *The vehicle manufacturer shall implement measures for the vehicle type to:*
(a) ***Detect and prevent cyber-attacks against vehicles*** *of the vehicle type;*
(b) Support the monitoring capability of the vehicle manufacturer with regards to ***detecting threats****, vulnerabilities and cyber-attacks relevant to the vehicle type;*

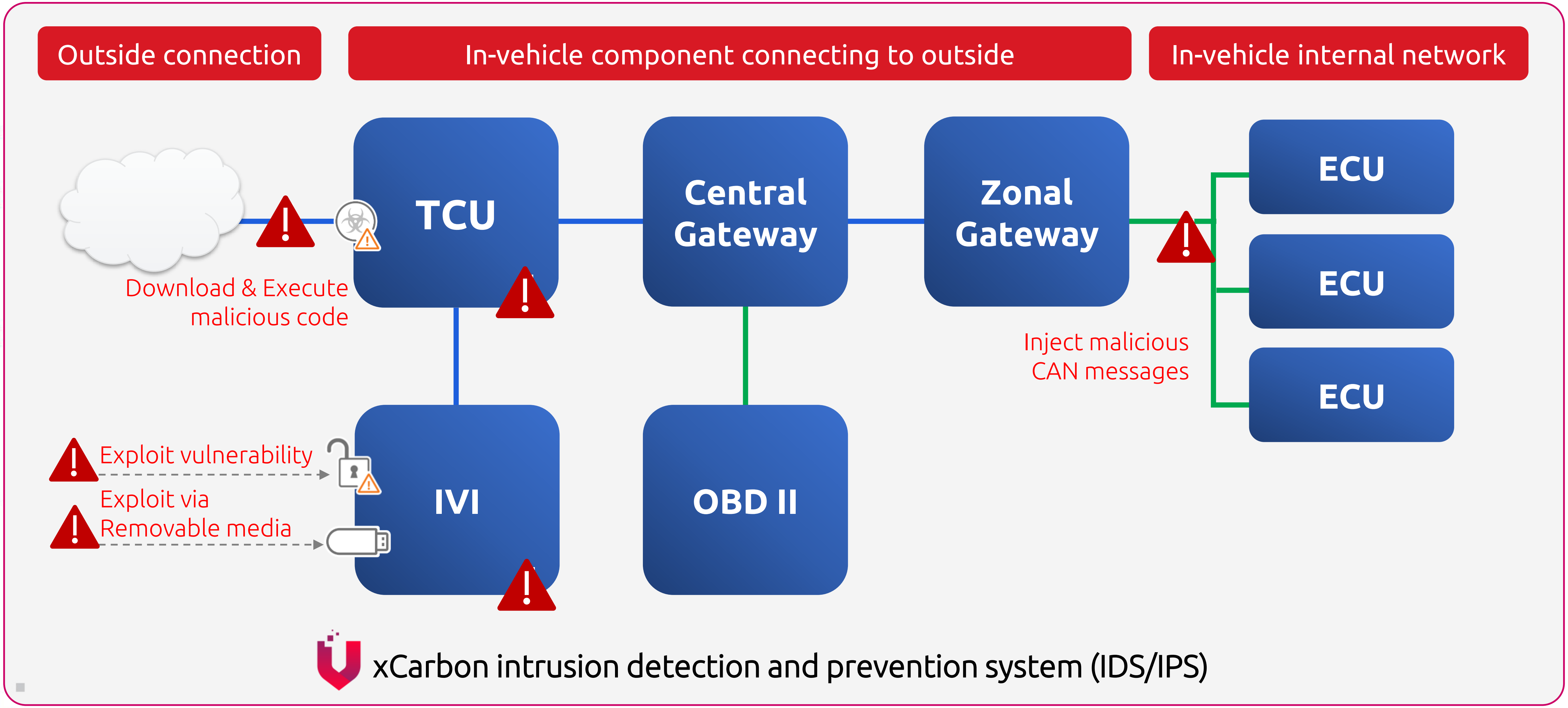
Annex 5

- ***M7*** *Access control techniques and designs shall be applied to protect system data/code.*
- ***M8*** *Through system design and access control it should not be possible for unauthorized personnel to access personal or system critical data.*
- ***M9*** *Measures to prevent and detect unauthorized access shall be employed*
- ***M13*** *Measures to detect and recover from a denial of service attack shall be employed*
- ***M15*** *Measures to detect malicious internal messages or activity should be considered*
- ***M21*** *Software shall be security assessed, authenticated and integrity protected.*
- ***M22*** *Security controls shall be applied to external interfaces*

Detection capabilities

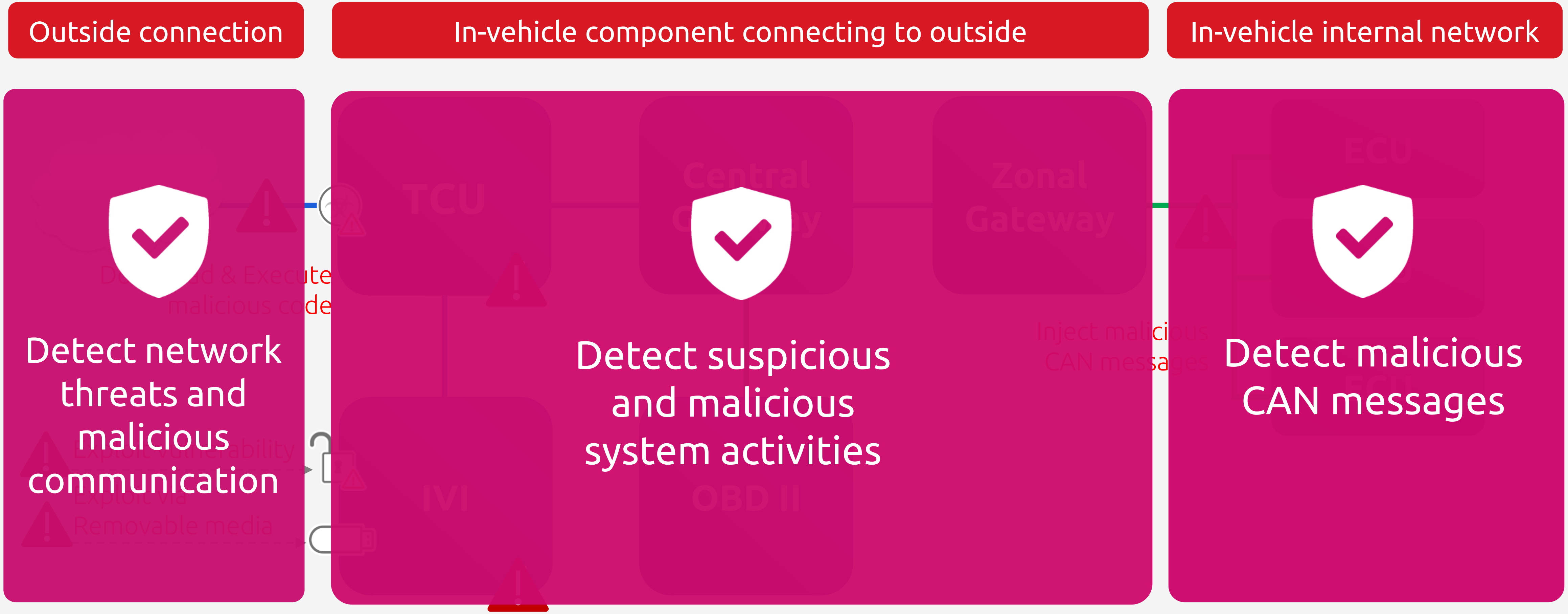
Detection mechanism

Protect your on-board ECUs from threats with our frictionless IDS/IPS


Outside connection
In-vehicle component connecting to outside
In-vehicle internal network
TCU
Central Gateway
Zonal Gateway
ECU
ECU
ECU
Download & Execute malicious code
Inject malicious CAN messages
Exploit vulnerability
Exploit via Removable media
IVI
OBD II

xCarbon intrusion detection and prevention system (IDS/IPS)

Protect your on-board ECUs from threats with our frictionless IDS/IPS



Outside connection

In-vehicle component connecting to outside

In-vehicle internal network

Detect network threats and malicious communication

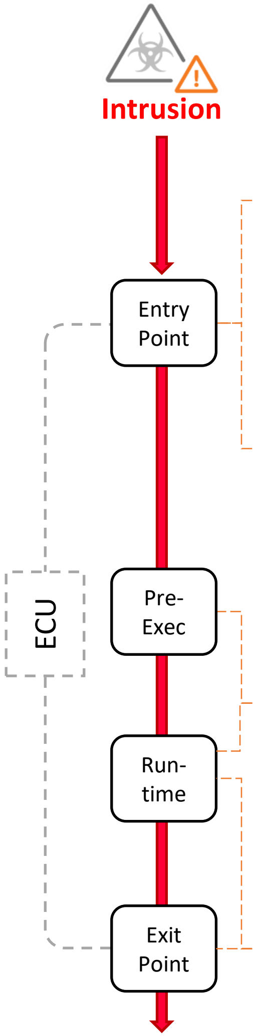
Detect suspicious and malicious system activities

Detect malicious CAN messages

Download & Execute malicious code
Exploit vulnerability
Exploit via Removable media
TCU
Central Gateway
Zonal Gateway
IVI
OBD II
Inject malicious CAN messages
ECU

xCarbon intrusion detection and prevention system (IDS/IPS)

Detection & Prevention



VicOne xCarbon host IDPS

Next-Gen Ethernet Firewall

- Identify suspicious events in Ethernet with Deep Packet Inspection, e.g., DoS attack
- Prevent network vulnerability exploitation with attack signatures (a.k.a. Virtual patch)

CAN Anomaly Detection

- Detect malicious CAN messages with rules generated by off-board ML
- Identify anomalies in ID, frequency and payload caused by attack

Advanced System Protection

- Ensure the software integrity and block the execution of unknown applications
- Detect unusual system activities and prevent system vulnerability exploitation (a.k.a. Virtual patch)

Intelligent Sensor

- Collects system activities and critical events for offboard analysis and data forensics
- Extract data from syslog, process log, network log with configurable filtering and aggregation

Mitigated Threats in UN R155 Annex 5

- 8.1 Sending a large number of garbage data to vehicle information system, so that it is unable to provide services in the normal manner
- 17.1 Corrupted applications, or those with poor software security, used as a method to attack vehicle systems

- 11.1 Malicious internal (e.g. CAN) messages
- 24.1 Denial of service, for example this may be triggered on the internal network by flooding a CAN bus, or by provoking faults on an ECU via a high rate of messaging
- 32.1 Manipulation of OEM hardware, e.g. unauthorised hardware added to a vehicle to enable "man-in-the-middle" attack

- 9.1 An unprivileged user is able to gain privileged access, for example root access
- 18.1 External interfaces such as USB or other ports used as a point of attack, for example through code injection
- 18.2 Media infected with viruses connected to the vehicle

- 7.2 Gaining unauthorized access to files or data
- 21.1 Unauthorized deletion/manipulation of system event logs
- 22.2 Introduce malicious software or malicious software activity

THANK YOU!

Kalli Schlauch – CEH, GCIH

VicOne

Driving Automotive Cybersecurity Forward