BOSCH PSIRT
#FIRSTCON22

ADAPTING PSIRT PROCESSES FOR THE AUTOMOTIVE B2B WORLD

TLP:GREEN

What I want to convey in this talk:

How the Automotive product environment differs from a typical Enterprise product environment and what this means for a (Tier 1) PSIRT working in that environment.

Current & future challenges.

Agenda

1. Introduction Bosch and its products
2. Introduction Bosch PSIRT
3. Introduction Automotive
4. So what’s so special about Automotive in a PSIRT context?
5. Adapting PSIRT processes for the automotive B2B world
6. Open Issues and future Challenges

Introduction Bosch

Our company in figures

In 2021

78.7

billion euros
sales revenue

3.2

billion euros EBIT
from operations

403,000

Bosch associates
worldwide at year-end
(approx.)

440

subsidiaries and regional companies in more than 60 countries

in ca. 25 business **divisions**

Introduction Bosch
Our business sectors

Mobility Solutions	Industrial Technology	Energy and Building Technology	Consumer Goods
~60%	~8%	~7%	~25%

Introduction Bosch
Bosch Products & Brands

BOSCH Service

BOSCH Diesel Service

itk ENGINEERING

BOSCH

ETAS

escrypt SECURITY. TRUST. SUCCESS.

Electro-Voice

JUNKERS Bosch Thermotechnik

DYNACORD

rexroth A Bosch Company

DREMEL®

Home Connect

Introduction Bosch PSIRT
Overview

Est. in 2016

BOSCH PSIRT
Product Security Incident Response Team

Security Incident Response:

- IR Processes coordinated with the Bosch divisions
- IR coordination at "the Bosch level"

Vulnerability Management:

- Coordinate VM across Bosch
- SPoC for Researchers / RDP
- Bosch Security Advisories via https://psirt.bosch.com
- Threat Information → Threat Intelligence (CTI)

Community Work:

- Foster climate for Responsible Disclosure
- IR/VM Communities
  (e.g. FIRST, Auto-ISAC)

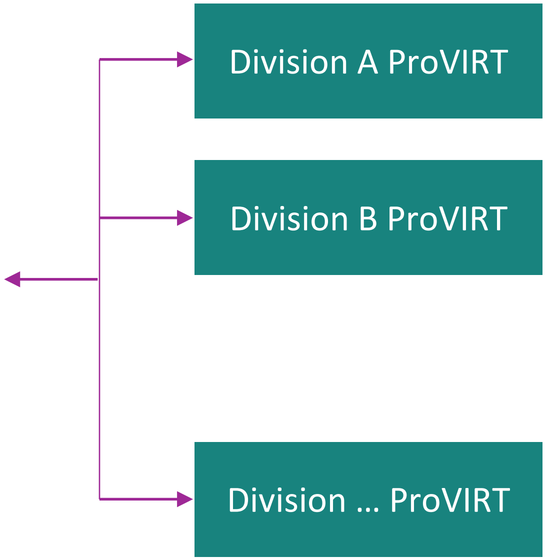
Introduction Bosch PSIRT

Bosch PSIRT – A ‘Coordinating PSIRT’

- Bosch PSIRT also acts as a ‘Coordinating PSIRT’ for roughly 25 divisions within the Bosch Group
- Close cooperation with each division’s ProVIRT (Product Vulnerability and Incident Response Team):

BOSCH PSIRT
Product Security Incident Response Team

- SPoC for researchers
- Coordination of VM and IR processes across Bosch
- Tool Chain, incl. psirt.bosch.com
- RDP and Security Advisories via psirt.bosch.com



Division A ProVIRT

Division B ProVIRT

Division … ProVIRT

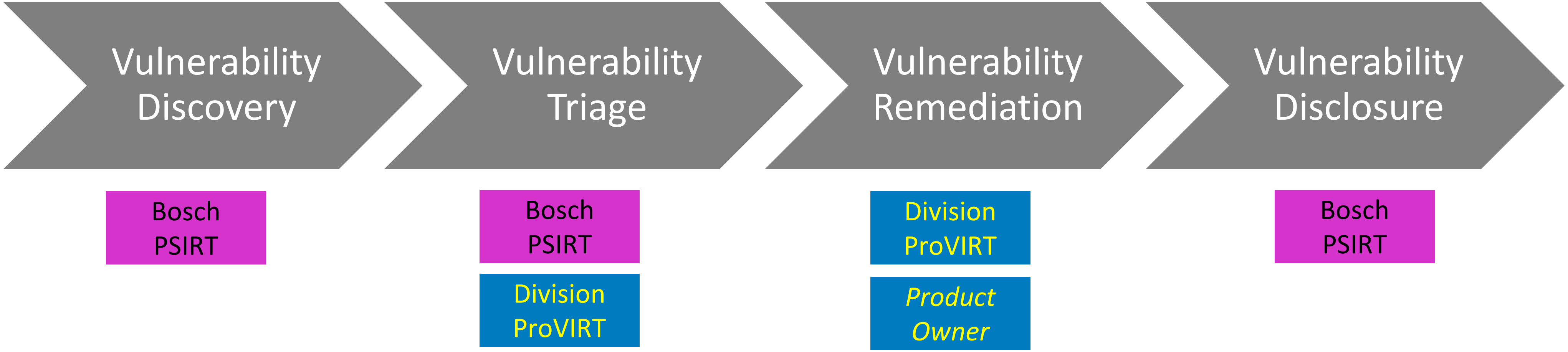
Roles in each division:

- ProVIRT
  - Security specialists for division’s products
  - Interface to engineering / software DEV
  - Coordination of division’s VM & IR processes
- Product Security Officer
  - Apply Security Engineering Process across the entire product lifecycle

Introduction Bosch PSIRT

Vulnerability Management Responsibility @ Bosch

Vulnerability Management process according to PSIRT Services FW:



Vulnerability Discovery

Bosch PSIRT

Vulnerability Triage

Bosch PSIRT

Division ProVIRT

Vulnerability Remediation

Division ProVIRT

Product Owner

Vulnerability Disclosure

Bosch PSIRT

Responsibilities in the Bosch VM environment

Introduction Automotive
Automotive context for the Bosch PSIRT

Automotive Glossary

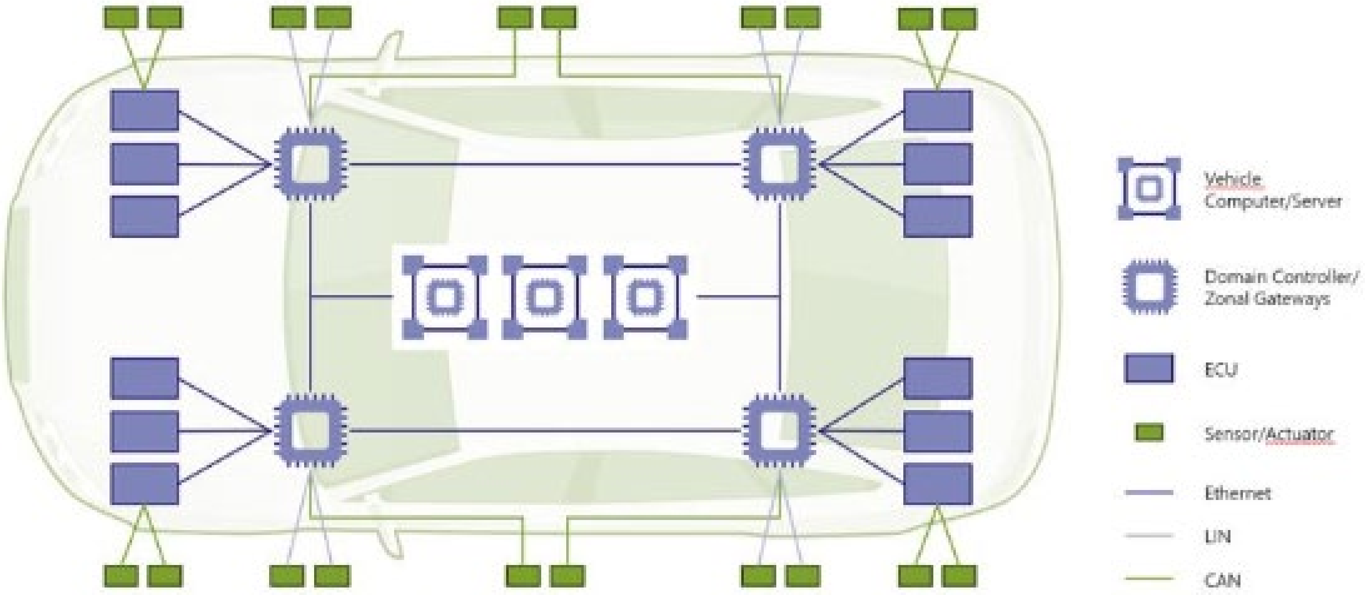
ECU – Electronic Control Unit: mini computers controlling various functions (~ 100-200 per vehicle)

Bus: in-vehicle network connecting devices - CAN, LIN, Flexray, Ethernet

E/E (electric/electronic) architecture: all ECUs, controllers, gateways, sensors, actuators in a vehicle connected via various in-vehicle bus systems

OEM – Vehicle Manufacturer

Tier – Direct or indirect supplier to the OEM: Tier 1 – Tier 2 – Tier 3

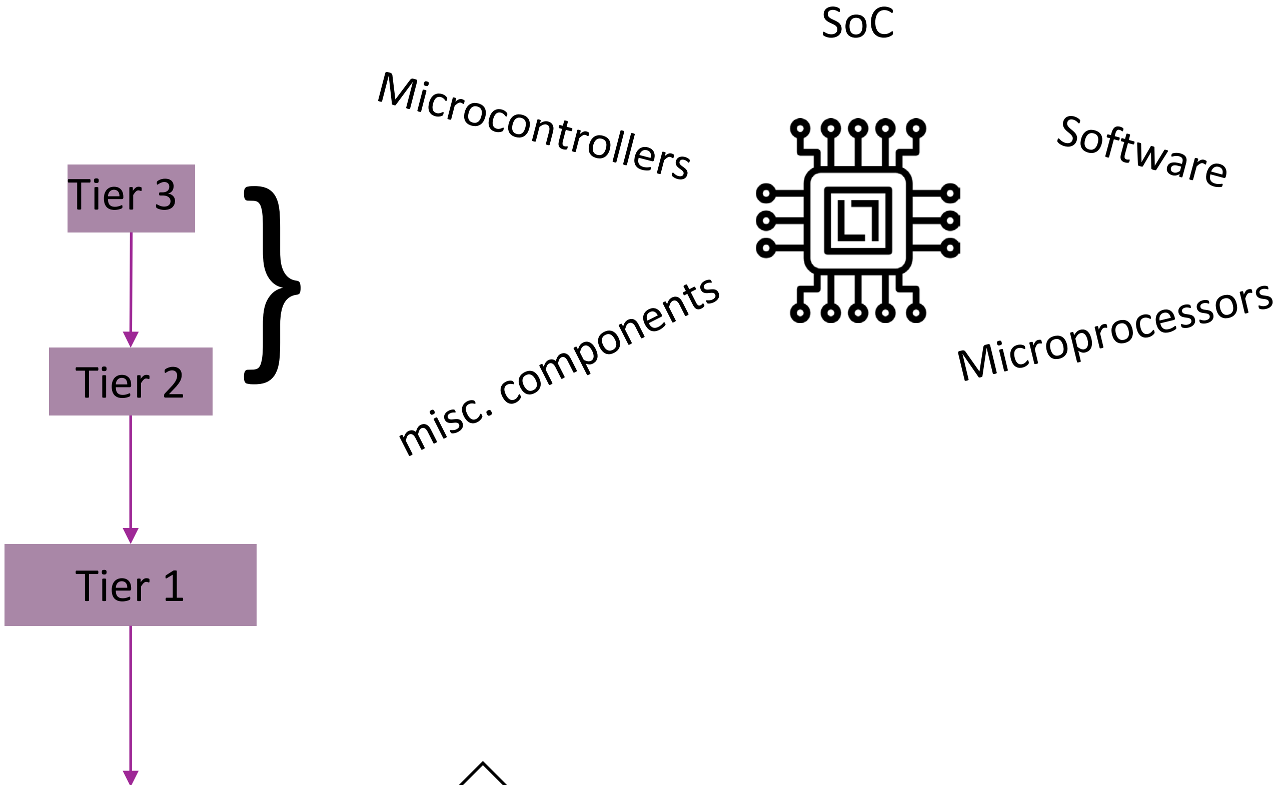


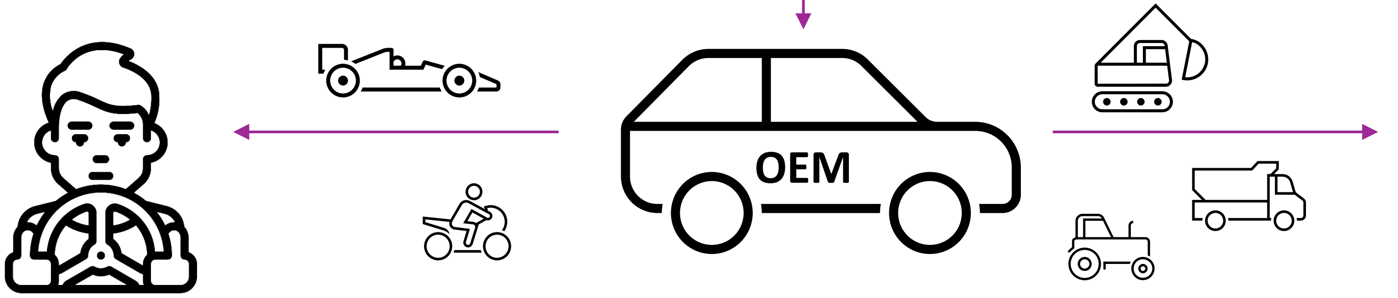
E/E Architecture Evolution:

‘Distributed’ → ‘Domain Model’ → ‘Vehicle-centralized’

Introduction Automotive

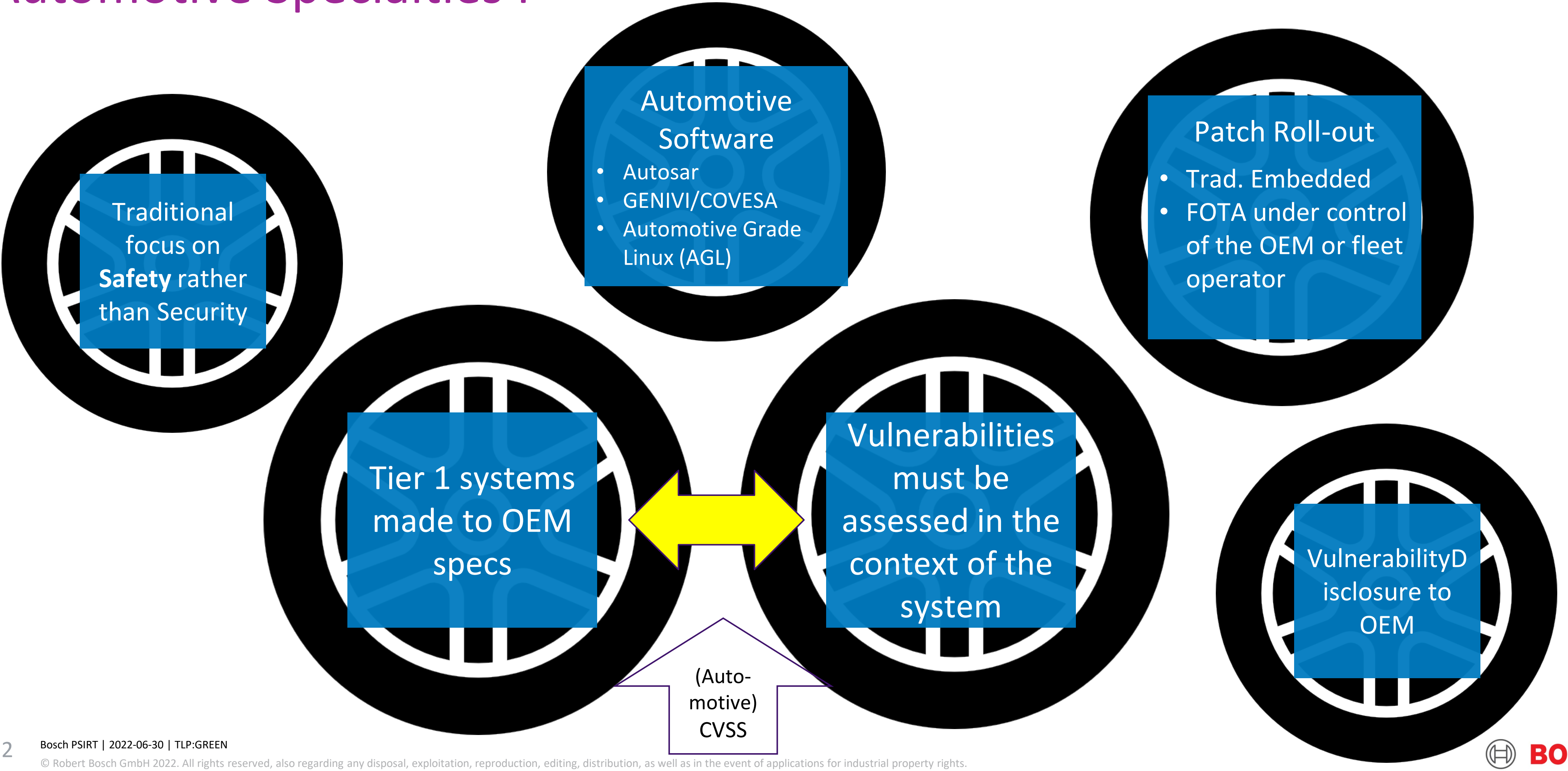
Automotive Supply Chain





So what’s so special about Automotive in a PSIRT context?

Automotive Specialties I



Traditional focus on **Safety** rather than Security

Automotive Software

- Autosar
- GENIVI/COVESA
- Automotive Grade Linux (AGL)

Patch Roll-out

- Trad. Embedded
- FOTA under control of the OEM or fleet operator

Tier 1 systems made to OEM specs

Vulnerabilities must be assessed in the context of the system

(Auto-motive) CVSS

VulnerabilityDisclosure to OEM

So what’s so special about Automotive in a PSIRT context?

Automotive Specialties II

Legislation:
- national
- UNECE R.155
- ISO/SAE 21434

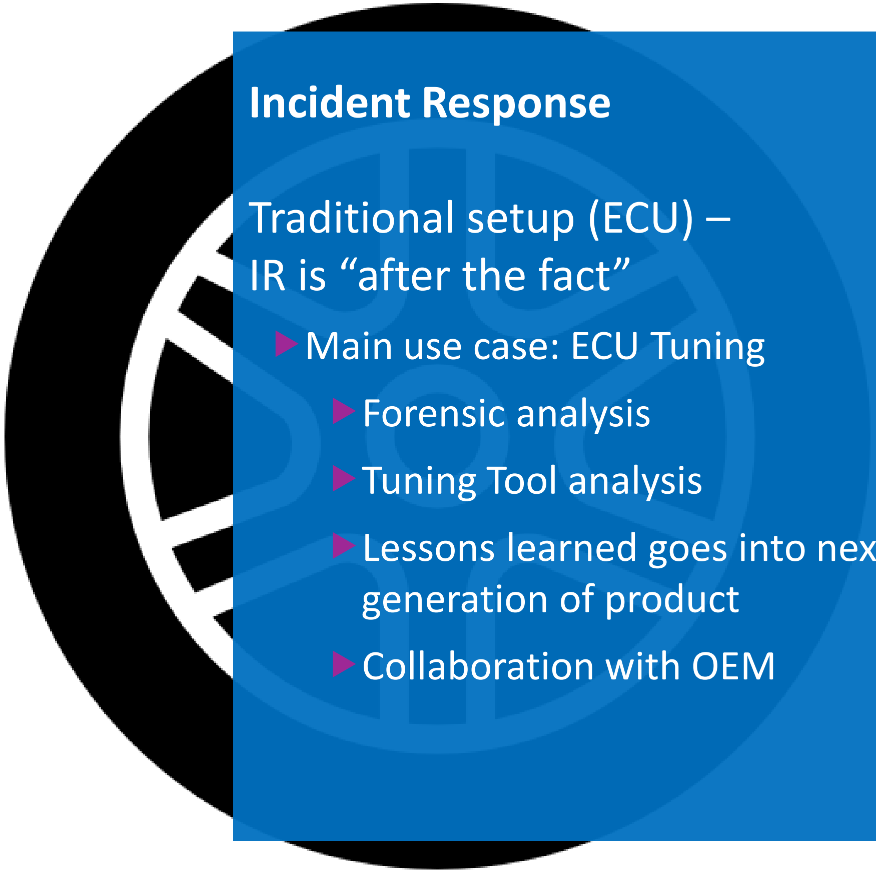
Security Community:
Auto-ISACs
(US/EU, JP, CN)

Security Research:
- individual
- academic
- commercial
- community
(e.g. ASRG)

- Jeep hack by Miller/Valasek – 2015
- Bosch Drivelog by Argus - 2016
- Various research on Teslas by Keen Labs
- Mercedes by Keen Labs – 2021
- Tesla by David Colombo

So what’s so special about Automotive in a PSIRT context?

Automotive IR - current



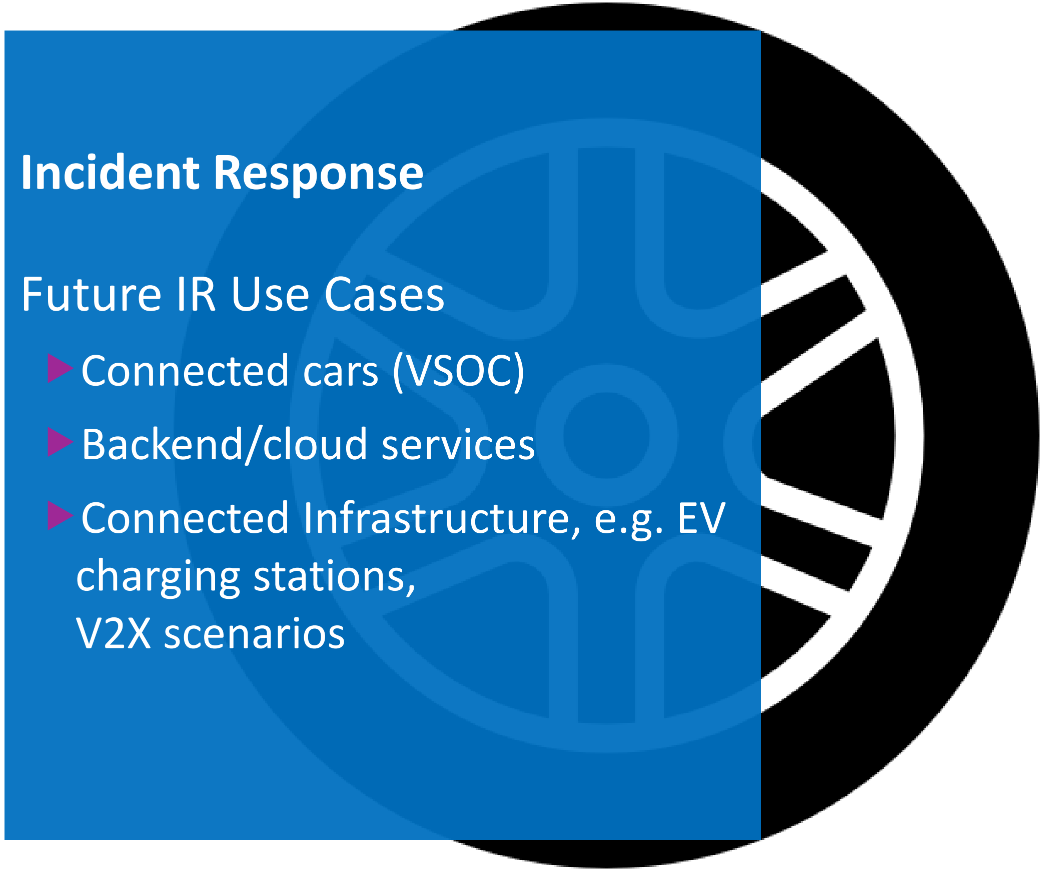
Incident Response

Traditional setup (ECU) –
IR is “after the fact”

- Main use case: ECU Tuning
  - Forensic analysis
  - Tuning Tool analysis
  - Lessons learned goes into next generation of product
  - Collaboration with OEM

So what’s so special about Automotive in a PSIRT context?

Automotive IR - future



Incident Response

Future IR Use Cases

- Connected cars (VSOC)
- Backend/cloud services
- Connected Infrastructure, e.g. EV charging stations, V2X scenarios

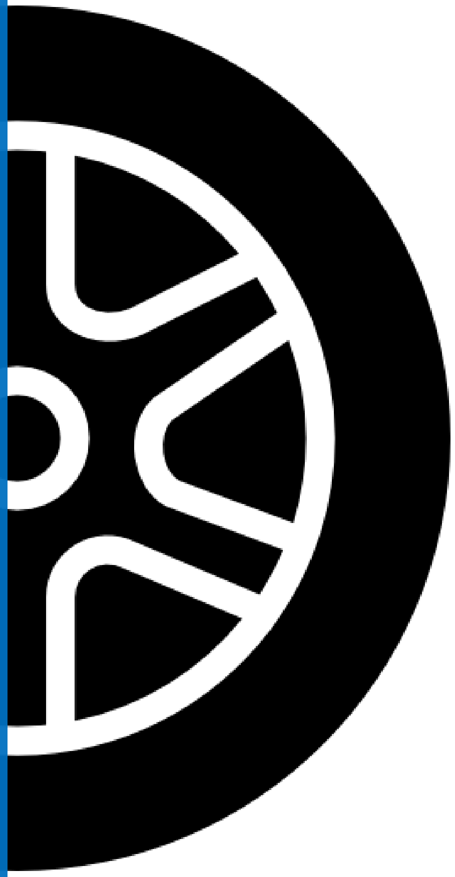
So what’s so special about Automotive in a PSIRT context?

Automotive VM

Vulnerability Management

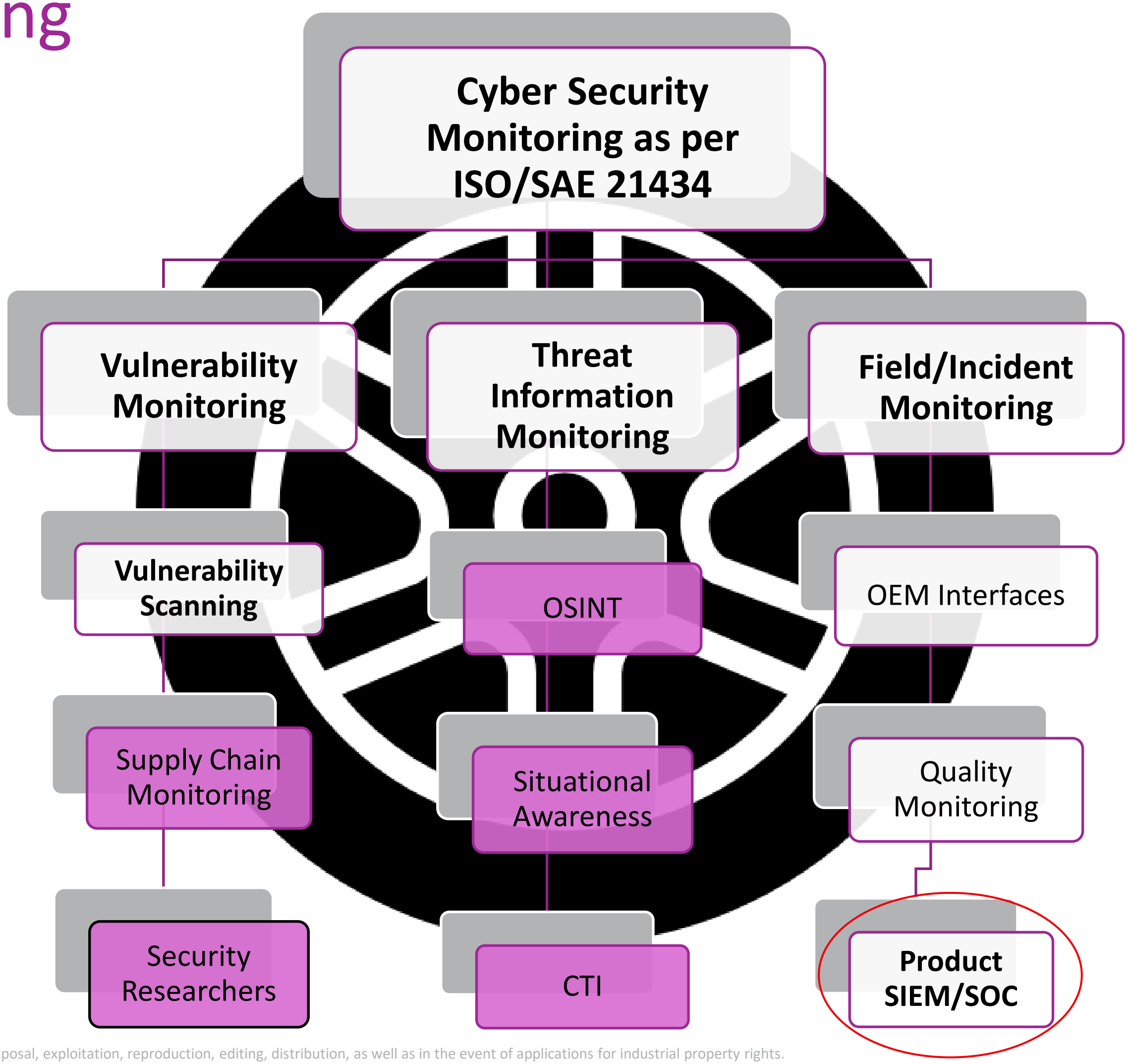
Embedded products

- No CVEs issued for ca. 90% of automotive
- => NVD is not the ultimate source for vulns
- **Cyber Security Monitoring** as per ISO21434
  - Hardware components & firmware (micro processors and controllers)
  - S/w components from other B2B vendors
- **Bosch Vulnerability Database**
  → Vulnerability Scanning and VM by the individual division
- **Direct Customer Communication**
  - Central OEM Communication
  - Project-to-Project



So what’s so special about Automotive in a PSIRT context?

Security Monitoring



Cyber Security Monitoring as per ISO/SAE 21434

Vulnerability Monitoring

Vulnerability Scanning

Supply Chain Monitoring

Security Researchers

Threat Information Monitoring

OSINT

Situational Awareness

CTI

Field/Incident Monitoring

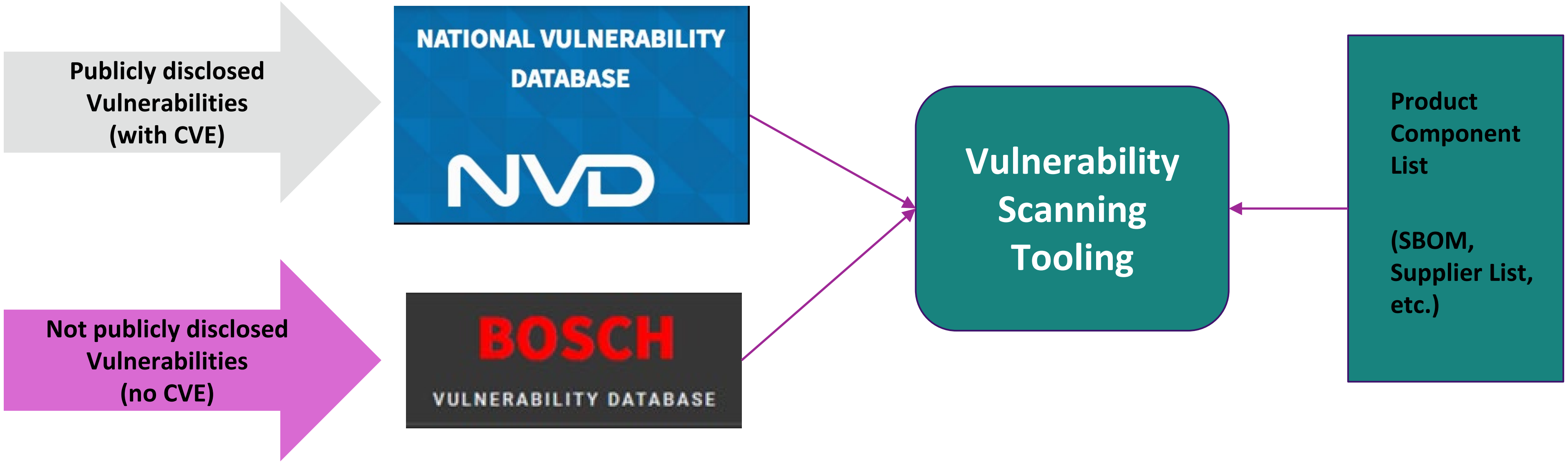
OEM Interfaces

Quality Monitoring

Product SIEM/SOC

So what’s so special about Automotive in a PSIRT context?

Vulnerability Scanning and the BVD



Publicly disclosed Vulnerabilities (with CVE)

NATIONAL VULNERABILITY DATABASE

NVD

Not publicly disclosed Vulnerabilities (no CVE)

BOSCH

VULNERABILITY DATABASE

Vulnerability Scanning Tooling

Product Component List

(SBOM, Supplier List, etc.)

Adapting PSIRT processes for the automotive B2B world

Summary: Special Aspects of Automotive PSIRT processes

Security Research:
so far conducted by
“advanced” researchers

Incident Response:
in ‘Embedded’ no direct containment possible
→ will change for connected components and services
(VSOC, FOTA)

Vulnerability Management:
□few CVEs
□Focus: Discovery via CyberSecMon
□customized BVD to enable automated scanning

Vulnerability Disclosure:
no Advisories, but “Centralized Customer Communication” and P2P

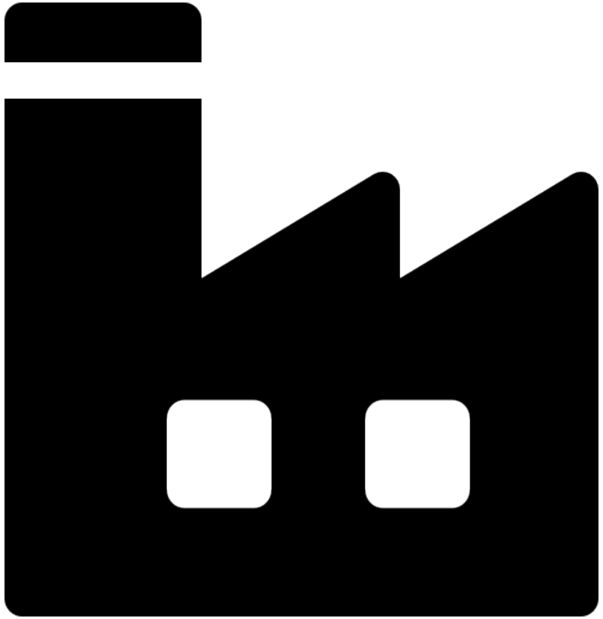
Adapting PSIRT processes for the automotive B2B world

Key learnings for other industries I

Applicability I:

Principles of Automotive Industry are by and large applicable to other B2B environments such as ‘Industry’ and ‘Building Technology’
→ ‘Integrator Business’

CVSS & CPE issues exist in other h/w-based product classes



Applicability of CVSS in its current form – Automotive-CVSS, *-CVSS

Unique identifier for hardware and firmware - CPE quo vadis?

Adapting PSIRT processes for the automotive B2B world

Key learnings for other industries

Applicability II:

As many traditional hardware-based products are developing into connected IoT-products, similar principles can be applied

=> Connected products consisting of h/w, app, and (Cloud) backend

Adapting PSIRT processes for the automotive B2B world

Key learnings for other industries

Convergence:

Convergence of product backends, Enterprise IT, and OT.

⇒ Opportunity for synergies and pooling of resources between SIEM/SOC, PSIRT, CSIRT, and OT-IR teams

⇒

BCDC

Automation of Vulnerability Scanning - SBOM, Tolling, Vulnerability Databases

Establish automated Advisory Exchange across all areas, e.g. CSAF

Adapting PSIRT processes for the automotive B2B world

Acknowlegements

- Wheel icon: https://www.flaticon.com/free-icon/alloy-wheel_226335
- Driver icon: https://www.flaticon.com/free-icon/driver_5283024
- Chip icon: https://www.flaticon.com/free-icon/microchip_1404247
- E/E Architecture schematic: courtesy and copyright of ETAS-escrypt
- Tier 1 info from: https://www.berylls.com/wp-content/uploads/2020/07/202007_BERYLLS_Study_Top_100_supplier-2019_EN.pdf

Thanks for listening!

Questions?

Now – or contact me via hans.ulmer@de.bosch.com