drivesec

we secure your things

drivesec

Webinar

How to build a test strategy for security assessment

July, 9th | 4.30 PM CEST
TEAMS

SPEAKER

Luca Ferrua
CTO at Drivesec

Session Topics

- Test framework
- Building Test Cases for Compliance
- Test Case Automation & Report Generation
- Drivesec as long-term Partner
- Drivesec Cyber Testing Community

drivesec

Test Framework

Vehicle

Attack vectors

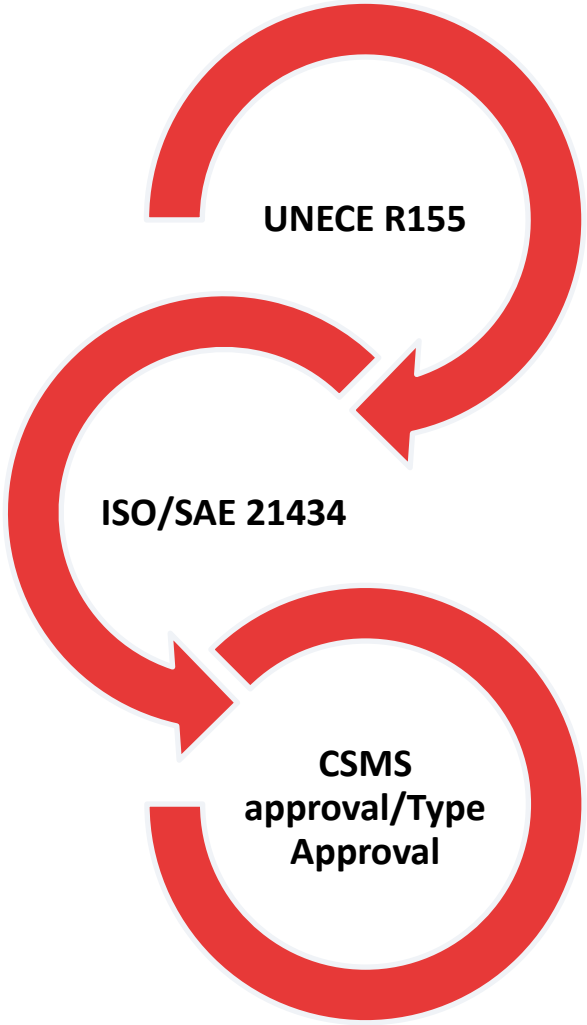
There are **big trends** towards digitalization vehicles, defined by being:

- **Autonomous**
- **Fully connected and OTA upgradable**
- **Software defined**

Vehicles need to be **resilient to cyberattacks and self-protecting**

Regulation Scenario

- ISO/SAE 21434 is used by OEMs organization to implement a process to be compliant with UNECE R155



- UNECE R155 introduces **Cybersecurity Management System** (**CSMS**) **at organization level**
- Needed interaction with the **whole supply chain**
- **Demonstration** of the existence of necessary **process**
- **Demonstration** of **technical evidence** to achieve the vehicle type approval

Cybersecurity assessment today…

OEMs and TIER1s are setting up processes and improving vehicle design in order to comply with regulation

Vehicle level penetration tests at the end of the design, is the choice of preference for most OEMs to certify and assess security posture

- Increasing homologation requirements
- Shorter development cycle and continuous sw update
- Complex logistic of benches, and parts

- Lack of skills and trained resources
- Shorter Time to market

Penetration Test (PT) on vehicle is not the most efficient way to validate security.

PTs are often costly activities, whose final value is strictly connected with the subject who will run them

PTs are in most case not replicable, inefficient, ensure a limited coverage

On vehicle sw and features, don't consider lesson learnt from previous vehicle model

Cybersecurity assessment

…new approach

- **Increase tests' reliability**, reduce logistics and costs and improve efficiency while assuring coverage of homologation requirements
- Be **integrated** with **proto vehicles**, **benches** and **HIL** systems. Testing on HIL is preferable to enlarge coverage of the security assessment
- **Continuous testing** processes that can integrate full testing automation
- **Reduce** the need of **human interaction**
- **Proactive** in **search** for vulnerability and implement a continuous learning process

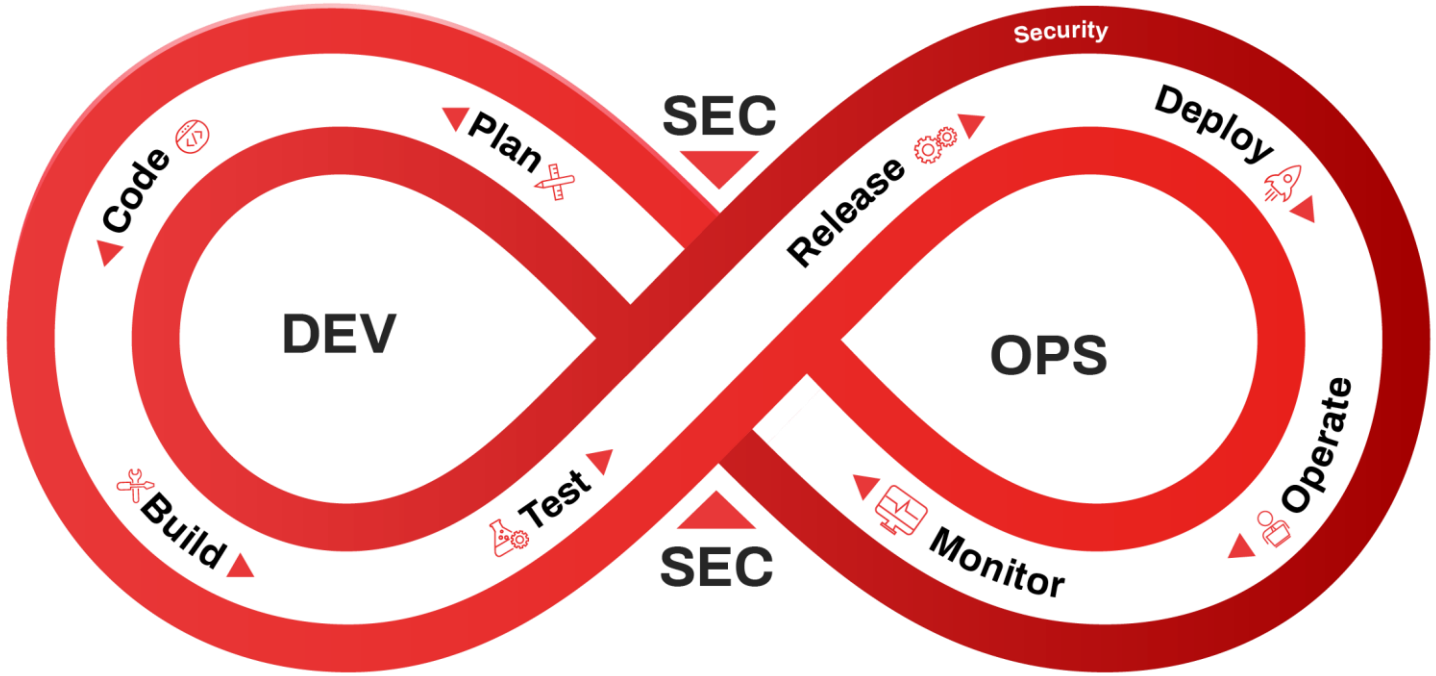
- Increasing homologation requirements
- Shorter development cycle and continuous sw update
- Complex logistic of benches, and parts

- Lack of skills and trained resources
- Shorter Time to market

drivesec

Building Test Cases for Compliance

Continuous Testing and Monitoring



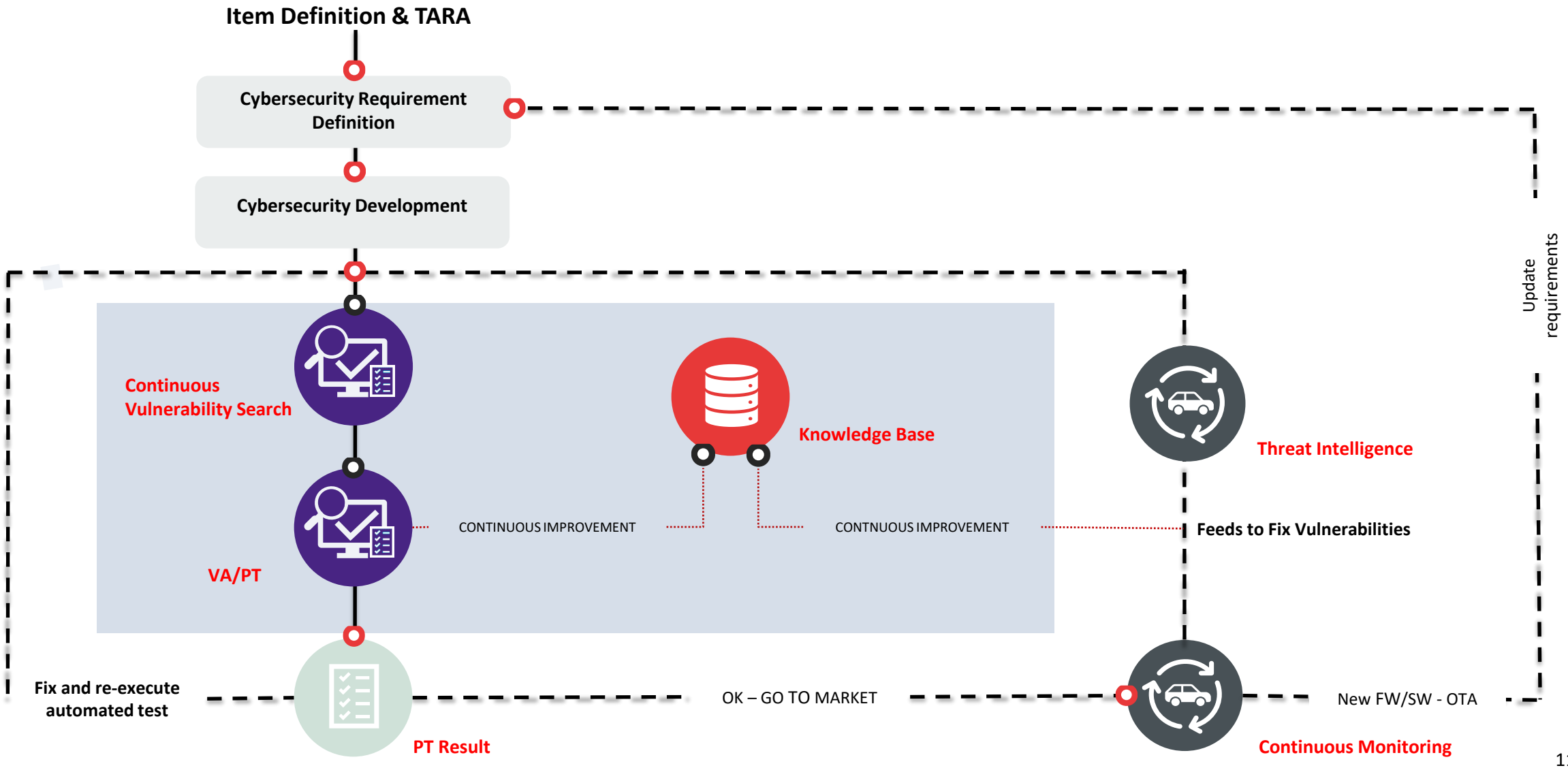
Continuous Vulnerability Search

VA/PT

Continuous Monitoring

Threat Intelligence

Continuous Testing Process



Continuous Testing Process

Item Definition

Item Definition	• A detailed description of the vehicle or component to be protected.
What is it included?	• Vehicle or components functions. • Interfaces & Attack surfaces. • Operational context.
Scope	• It’s the input of the TARA.

Continuous Testing Process

TARA

TARA (Threat Analysis and Risk Assessment)	• The process of identifying and evaluating threats and risks associated with the vehicle or component to determine the necessary security measures.
What is it included?	• Damage scenario impact. • Attack tree methodology.
Scope	• The output is a list of Cybersecurity Goals (High-level requirements).

Continuous Testing Process

Cybersecurity Requirement

Cybersecurity Requirement Definition	• Starting from Cybersecurity Goals, requirements and specification security measures needed to protect the system against identified threats are extracted.
What is it included?	• Development requirements and guidelines for product development.
Scope	• Definition of rules to apply to mitigate risks and threats.

Continuous Testing Process

Cybersecurity Development

Cybersecurity Development	• Implementing security measures in a vehicle or component, ensuring that security is integrated at every stage of product development, using the requirements and specifications previously identified.
What is it included?	• SW architectures, piece of code.
Scope	• Create an environment that allows production functions to work with the expected security level.

Continuous Testing Process

Vulnerability Search

Continuous Vulnerability Search	• Ongoing activities to monitor and search for new vulnerabilities in vehicle or component to prevent potential attacks and ensure the vehicle's security throughout its lifecycle.
What is it included?	• List of test case to cover requirements. • Test plan.
Scope	• Make a clear status of cyber security development at early stage to correct and improve the full system.

Continuous Testing Process

Penetration Test

Penetration Test	• Activities performed by security experts to identify and exploit vulnerabilities in the vehicle or component, assessing the effectiveness of implemented security measures.
What is it included?	• Test plan. • Scenarios of attack.
Scope	• Test system resilience to cyber attacks.

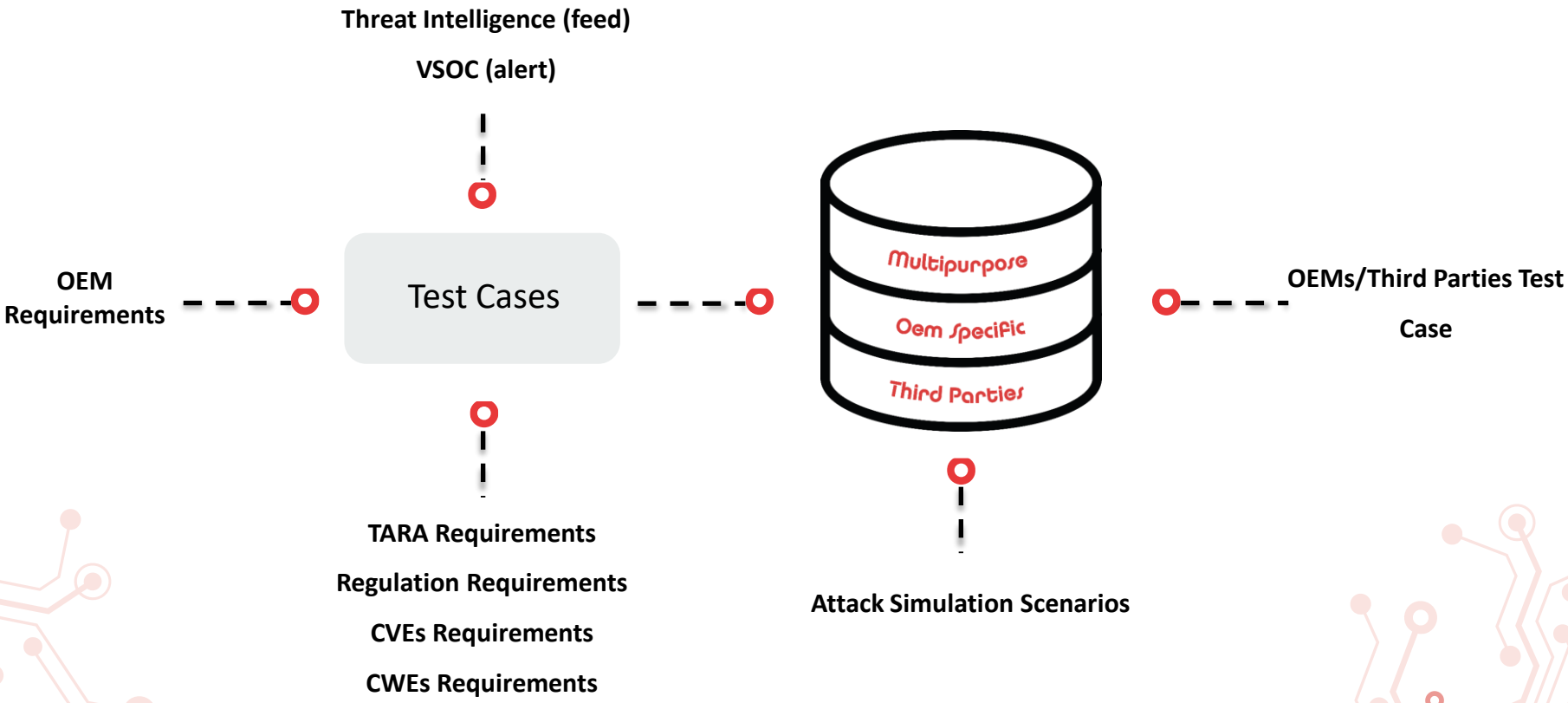
Continuous Testing Process

Penetration Test Result

Penetration Test Result	• The outcomes of penetration tests that highlight found vulnerabilities, their potential impacts, and recommendations for improving system security.
What is it included?	• List of Vulnerability. • List of Warnings. • Discovering of attack paths.
Scope	• Identify all vulnerabilities and security malfunctions to be corrected before releasing products or product update on the market.

Continuous Testing Process

Cybersecurity Knowledge Base



Continuous Testing Process Test Case

Test Goal & Regulation

- Clear description of the test scope.
- Regulation mapping (e.g. threats listed within the Annex 5 of the UN 155 regulation).

Expected Result

- Definition of the expected behaviours and expected result in case of successful execution.

Test setup

- Description of the main steps useful for test case execution.

Target

- Attack surfaces (e.g., In vehicle networks, wireless networks,…).

Test Category

- Categories according to the type of test goal (e.g., reconnaissance, fuzzing, DoS, ...)

Vulnerability & Threat Classification

- Real cyber attacks against vehicles and ECUs
- Vulnerabilities publicly disclosed.
- Evaluation according to the STRIDE and CIA threat models.

Scripts

- Concrete implementation of a specific test case that can be executed to assess a specific item.

Test Case Example

drivesec

Test Goal

- Verify if the ECU makes use of the best practices to reduce the effectiveness of brute force attacks against diagnostic access authentication.
- Reference UNECE R155 Threats Annex 5
  - “An unprivileged user is able to gain privileged access to vehicle systems)
  - “Cryptographic technologies can be compromised or are insufficiently applied”

Expected result

- Target ECU enforces a time delay when one or more authentication attempts have failed.

Test Setup

1. Identify the pinouts related to the target network
2. Connect the pins to HW adapter/converter

Target

- Attack vector: ECU diagnostic stack

Test category

- Spoofing
- Brute force

Vulnerability

- CVE-2017-14937
- **CIA**: Integrity
- **STRIDE**: Spoofing & Escalation of Privilege

Continuous Monitoring Process

Reporting & Monitoring

The output of the test can be used to

- Collect information to demonstrate that risks are identified and managed
- Document Risk Assessment reports
- Submit to the Approval Authority all evidence for achieving Certification
- Detect appropriate Cybersecurity measures
- Detect and respond in advance to possible cybersecurity attacks
- Write and share lesson learnt and improve organization processes

drivesec

Test Case Automation

WESETH®: IoT Cybersecurity Testing Platform - Overview

Weseth® by drivesec

EFFICIENT

AUTOMATED

AUTONOMUS

REMOTE

ITALIAN PATENT
 # 102020000032882

Patents requested in EU andUSA
PCT/IB2021/062463

WESETH® Remote Tool for Cyber Researcher (1.0)

WESETH® Test Automation tool for validation engineer (2.0)

WESETH® Cybersecurity Knowledge Base builder

WESETH® Remote Management

ONE STOP SHOP FOR CYBER SECURITY CERTIFICATION AND TESTING

WESETH®

Service for Cyber Researcher

WESETH® Remote Tool for Cyber Researcher (1.0)

Engineering tool to **execute the remote operation on a System Under Test** (SUT) that is not provided with a secure remote interface.

The best application is to run a **full systems Penetration Test from remote.**

Allows remote operators to work remotely on a secure connection on the SUT.

Fully autonomus

Low cost

Easy to install (not interfere with Customers' ICT infrastructure)

Cybersecurity Engineer

Bug Bounty operators

Validation Engineer

WESETH®

Service for Automated Testing

WESETH® Test Automation tool for validation engineer (2.0)

Full **cloud-based**, testing **automation tool**.

Enable **automatic verification of requirements**, simulation of **attacks**, **spoofing** of information and **fuzzing** of systems and networks.

Based on the WESETH® Knowledge Base

Database of Scritps, that can be executed on the WESETH® Box.

WESETH® Knowledge Base is a list of scripts that can be enriched by Customers

WESETH®

Increase company Know-how

WESETH® Cybersecurity Knowledge Base (KB) builder

Allow the **management**, throughout the Company, of **cybersecurity knowledge and lessons learnt**.

KB is a collection of test scripts.

Every script can represent a requirement test, a fuzzing tool or an attack simulator.

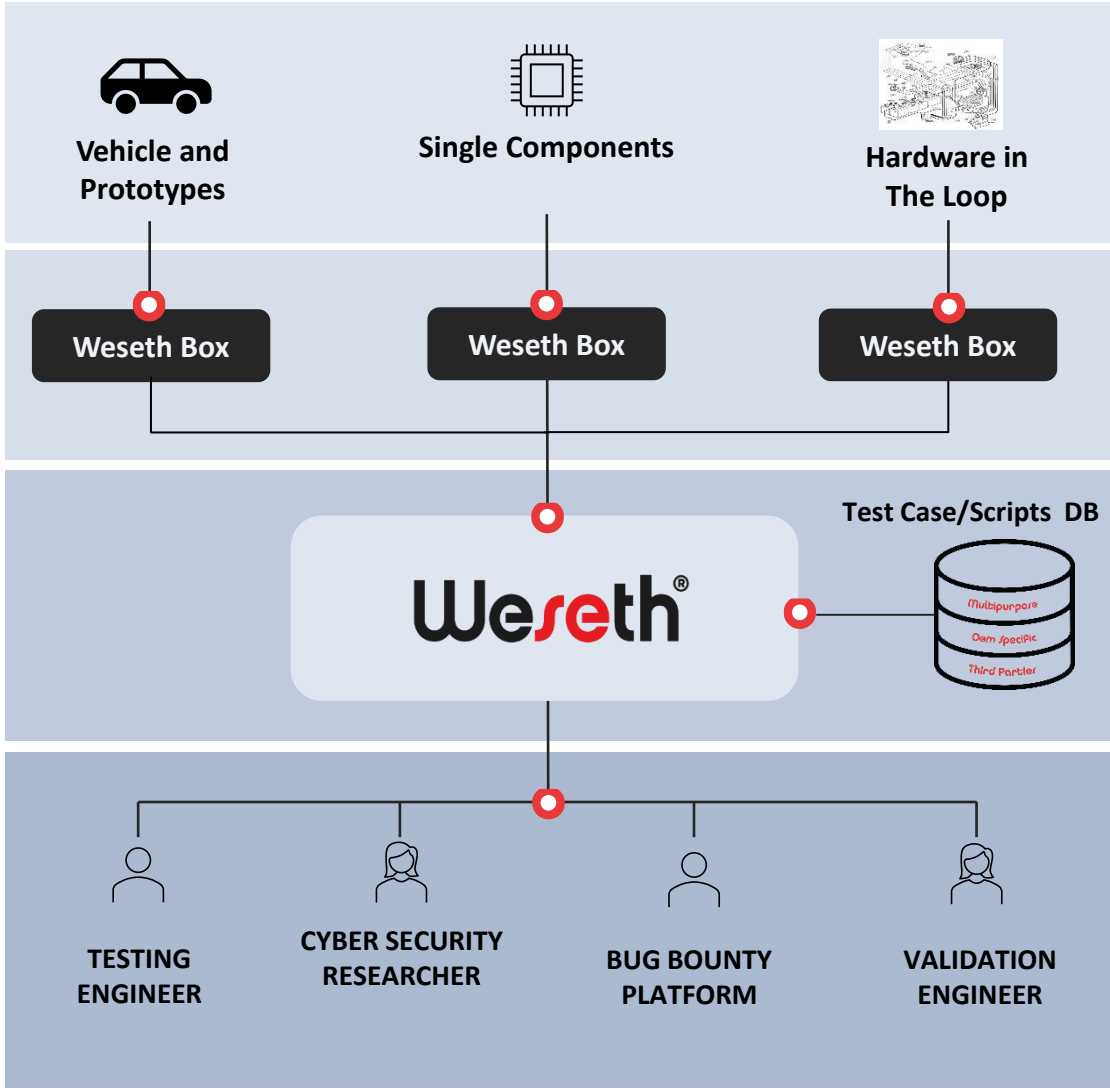
KB grows with the experience and increase the coverage of the Vulnerabilities Assessment.

KB builder is also the base of the execution of automated test

WESETH®: Remote and Automated Testing

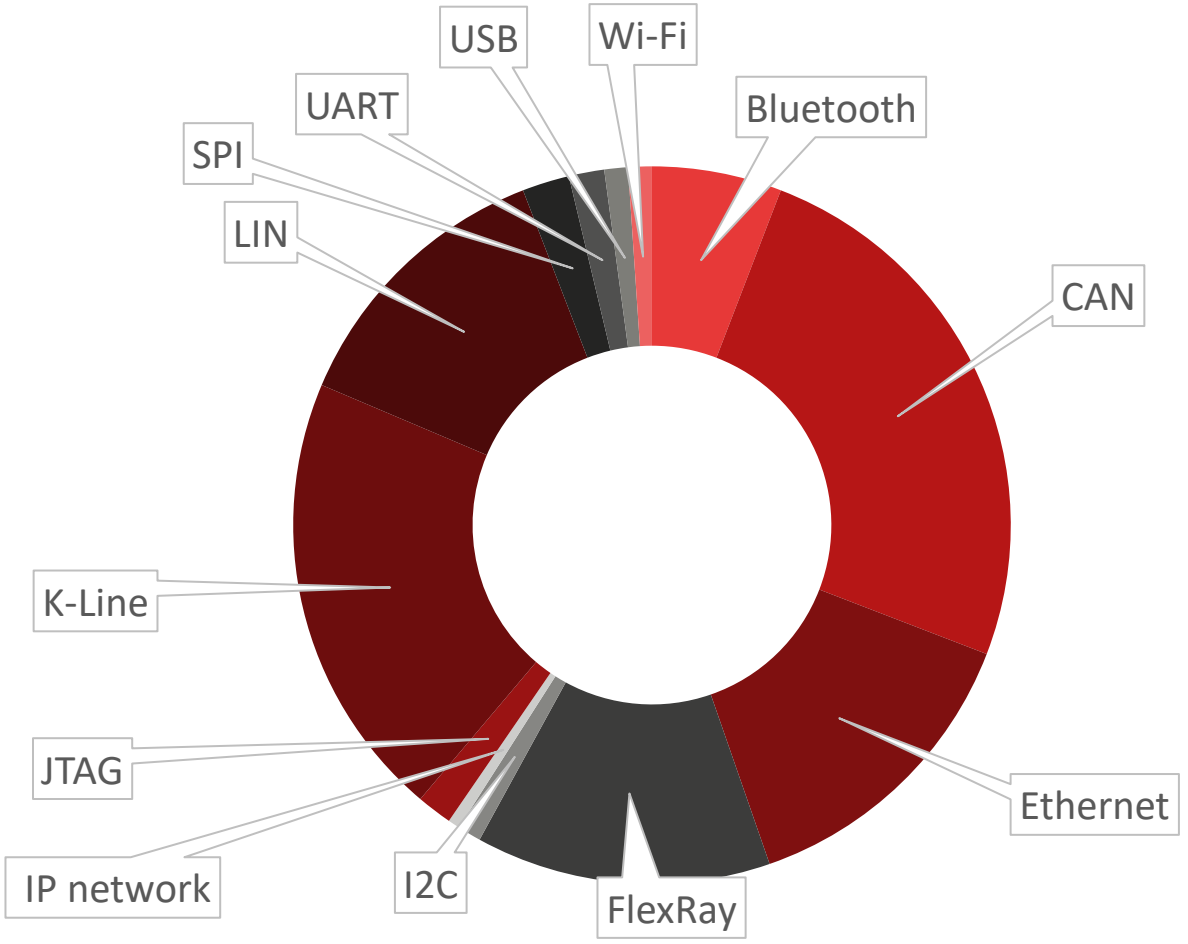
drivesec

Platform for Remote Engineering & Testing
of components and system requirements (including security)



- **Customer hardware remains with the customer**
  ECU, vehicle, sub-system, Hardware in the Loop systems …
- **The customer attaches Weseth remote box to the target hardware which shall be tested / validated**
  Physical connection via CAN/CANFD/ETHERNET, Bluetooth, USB, streaming of video, multiple Digital IOS.
- **Cloud Based server manages the secure integration between System Under Test and remote Users**
  Test Case and Scripts are stored in a safe environment and are automatically loaded on the Boxes when needed
- **Test Engineers describe the system under test;** based on this, Scripts are automatically selected and loaded on the respective Box for automatic execution
- **Remote Users can access the system under test** to perform penetration tests, emulate attacks, verify requirements and collect data

Test Case Coverage



drivesec

“Drivesec as a long term Partner”

Drivesec Supports & Solutions

OEMs/Tier1s Duties

- Test case Requirements VS UNECE R155
- Validation Assessment
- Penetration Test
- Cybersecurity Requirements elicitation
- Prepare documentation ISO 21434
- Process Desing (SUMS, CSMS)

What Drivesec can deliver

- UNECE R155 test cases documents covering Annex 5 and more. Test cases can be used to build a test plan
- Set of scripts to test all test cases. Scripts are fully automated by the WESETH platform and can be integrated with HIL systems.
- Remote execution of Pen Test via WESETH platform integrated with HIL systems. Drivesec delivers to Customers the scripts specifically prepared for them
- Requirements extraction (own TARA tool)
- Templates kit for all Work Products
  Training and support in document preparation
- Consulting on document preparation (framework documents available)

drivesec

Drivesec CyberTestCommunity

Drivesec CyberTestCommunity

Drivesec is launching a **test community**, with the aim to share information material, tutorials, insight and software tools regarding automotive and IoT product security posture assessment.

The community will be **launched** in **September 2024**. Drivesec is opening **subscriptions** from **July 2024**.

Participants will receive a regular newsletter and will have access to a reserved area in the Drivesec portal, with resources that help **to become more efficient in testing automotive and IoT systems**.

The community is dedicated to test and validation engineers, regardless of their level of knowledge about cybersecurity

Be among the first to Join the community through our page
https://www.drivesec.com/resources/join-the-cyber-test-community/

Thanks for your attention

For any further info, please, do not hesitate to contact

marketing@drivesec.com