TechWorks AI

Launchpad

Bletchley Park

Milton Keynes

16th April 2024

UKRI Innovate UK

BridgeAI

Feasibility Study of Generative AI in Automotive Cybersecurity Threat Modelling

16 April 2024

Company - Secure Elements Ltd

Automotive Cybersecurity Engineering Software Company

- ✓ Founded – Jan 2022
- ✓ Mission – Help In Shaping *Safe and Secure* Future Mobility
- ✓ We Build Engineering Tooling Products
  - ✓ CRISKLE – Integrated Product Security Lifecycle Application
  - ✓ CRISKLE MSoC – Mobility Security Operations Centre

Mr. Saket Mohan

Founder & CEO

Proud Members Of

CYBER RUNWAY GROW by plexal ALUMNI

AESIN AUTOMOTIVE ELECTRONICS INNOVATION

ITS United Kingdom Better transport through technology

AUTO-ISAC Auto Isac

ASRG

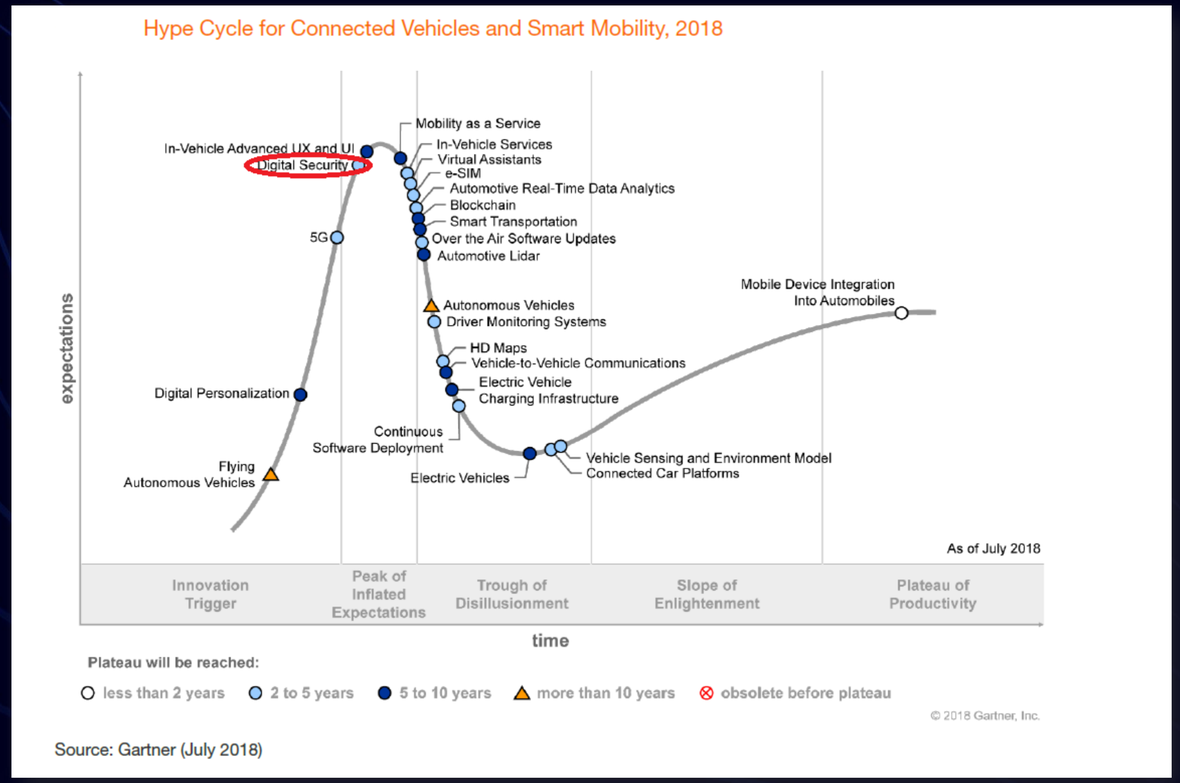
Feasibility Study

GenAI in Automotive Cybersecurity Threat Modelling

Project Name	GenAI in Automotive Cybersecurity Threat Modelling
Project Number	10080056
Start Date	1st Oct 2023
End Date	30th March 2024
Project Funding	GBP 50,000 (Grant) Sector - Transport
Funding Agency	Innovate UK
Project Partners	Secure Elements Ltd (Lead) Swansea University Techworks (AESIN)

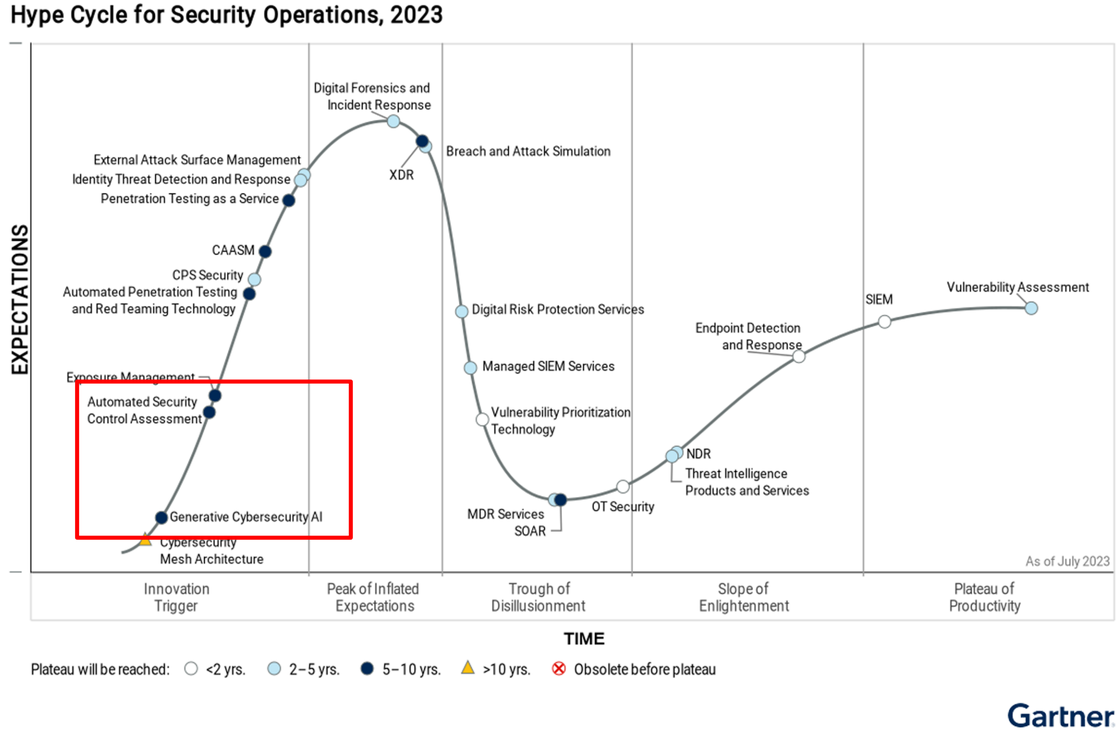
Automotive

Cybersecurity Hype Cycle



Source: Gartner (July 2018)

Figure 1: Hype Cycle for Security Operations, 2023



GenAI led cybersecurity solutions for automotive are an innovation trigger

Automotive Cybersecurity

Today

Partially Connected Human Driven Cars

Transition

+ 3 to 5 Years

CASE | C - connected, A - automated, S - shared, E – electric

Software Defined Vehicles Governing Safety

Transition to **Software Defined Connected Vehicles** brings Substantial Safety, **Security** And Liability Risks For Automakers

Cybersecurity Attacks on Rise

Mobility companies have seen an exponential rise in automotive cybersecurity attacks

Aug 2023– Mercedes-Benz

Dec 2022– NIO

Apr 2022– HYUNDAI

Feb 2021– TESLA

Aug 2020– KIA

2019– PEUGEOT, Volkswagen, Ford, TESLA, Honda

2019– TOYOTA

2017– BMW, HYUNDAI

Renault, NISSAN

Is YOUR car safe? Jeep hackers that prompted recall of 1.4 million vehicles show off new hack to take control at high speeds

- Sent false messages to its internal network, overriding the correct ones
- Were able to make vehicle unintentionally speed up, or slam on its brakes
- Hackers now work for car service Uber

Security

Security bugs let these car hackers remotely control a Mercedes-Benz

Zack Whittaker @zackwhittaker / 11:00 PM GMT+1 • August 6, 2020

Comment

Tech

Hackers crack Tesla software to get free features

Premium in-car features include Full Self-Driving and heated seats

Anthony Cuthbertson • Monday 07 August 2023 18:49 BST • 3 Comments

UK Halts Sale of Electric Vehicle Charger Over Cybersecurity Fears, Raising National Grid Concerns

Regulations

Is driving compliance & is a legal requirement

Every automotive organization requires a well-established Cybersecurity Management System [CSMS]

INCOMING REGULATIONS

Non-compliance means

UNECE July 2024

China GB/T 2025

India (AIS 189)

Home / News / VW kills off its cheapest electric car over cybersecurity rules

VW kills off its cheapest electric car over cybersecurity rules

By dpa | 21 October 2023

Porsche To Kill ICE-Powered Macan In Europe Over Cybersecurity Laws

Porsche's best-selling model will be discontinued from markets within the European Union in spring of 2024

by Thanos Pappas December 15, 2023 at 08:29 22

Ok, so what's the Problem ?

Conducting Cyber Risk Assessments – Tooling

Excel Based TARA Tools for Threat Modelling

Lack of experienced personnel to conduct TARA Assessments

Significant/continual human effort required to conduct TARA on >60 ECU's /Vehicle

Result

TARA becomes a **STATIC** document

- With fixed <limited> number of assets and threat scenarios
- Requires significant labor <labor intensive>
- Only covers bear minimum attack vectors
- Manual effort required to relate Threat Scenario's and Mitigation

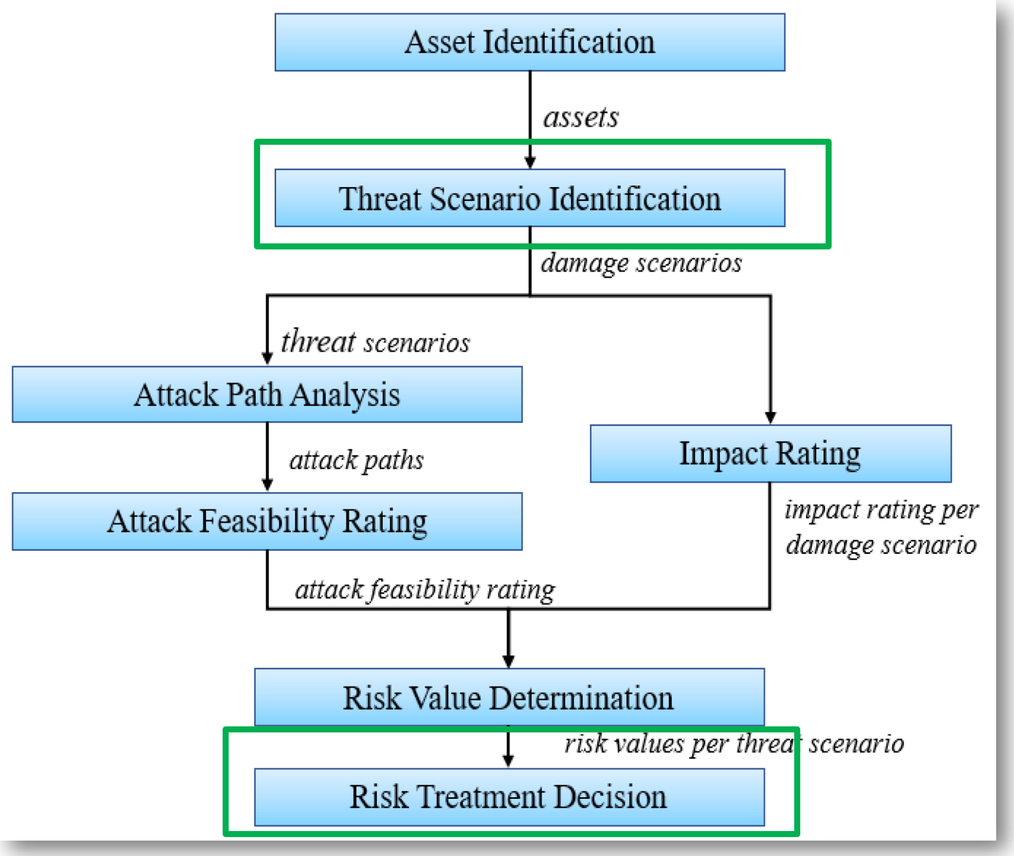
Overall, leading to incomplete TARA documents resulting in increasing vulnerabilities and exposed attack surfaces.

TARA – Threat and Risk Assessment (ISO/SAE 21434)

ISO/SAE 21434 based TARA

Threat Modelling Steps

Threat modelling comprises six essential steps
- Assets [SW, HW, Data etc]
- **Threat Scenario generation for the Asset [CIA Triad compromise of Asset]**
- Attack Path Feasibility Rating
- Impact Rating
- Risk Determination and
- **Mitigation Strategies**



Datasets for Training

Cybersecurity Pre-Labeled Data

Detection using Open-Source vehicle dataset

Training of Text based Model using CRISKLE data

Integration in CRISKLE

Dataset	Real/Synthetic	Attacks	DoS	Fuzzing	Replay	Spoofing	Suspension	Masquerade	Benign duration	Attack duration	Labeled
HCRL CH	Real	4	✓	✓	-	✓	-	-	0h 8m 20s	7h 21m 57s	Yes
HCRL OTIDS	Real	3	✓	✓	-	-	-	✓	0h 17m 17s	0h 18m 56s	No
HCRL SA	Real	9	✓	✓	-	✓	-	-	0h 3m 31s	0h 8m 53s	Yes
HCRL CHDC	Real	4	✓	✓	✓	✓	-	-	-	0h 23m 23s	Yes
SynCAN	Synthetic	5	✓	✓	✓	✓	✓	-	-	-	Yes
TU Eindhoven	Synthetic	5	✓	✓	✓	-	✓	-	0h 19m 20s	0h 8m 17s	Yes
ROAD	Real	13	-	✓	-	✓	-	✓	3h 0m 32s	0h 27m 10s	No

Scenario Set Up Parameter	Value
Data Set Name	Real ORNL Automotive Dynamometer (ROAD) CAN Intrusion Dataset
Type of Bus System	CAN
Number of Attack Captures in Dataset	13
Number of ECU's in dataset	106
Total Time of recorded dataset - Attack	30 minutes
No. Of Ambient captures	12
Attack Types	Fuzzing, Spoofing and Masquerade
Attack Nature (CIA) property	Authenticity, Integrity

ROAD – ORNL - https://zenodo.org/records/10462796

Model Training – Trial 1

Threat Scenario Generation using LLM without any system context data

Detection using Open-Source vehicle dataset

↓

Training of Text based Model using CRISKLE data

↓

Integration in CRISKLE

☹

Input Threat Scenario

```
# Generate a new threat scenario
seed_text = 'An attacker disables the eCall functionality'  # Replace with your actual seed text or ID
new_scenario = generate_scenario(seed_text)
```

Generated Scenario

```
Setting `pad_token_id` to `eos_token_id`:50256 for open-end generation.
An attacker disables the eCall functionality but only if it hasn't been installed.
Therefore, for any call that is not installed, calls with the "id" parameter should be sent to the attacker via the CallPolicy object,
, which will then attempt
```

Output :

- Incomplete Threat scenario
- Random in nature // Hallucinated
- No context

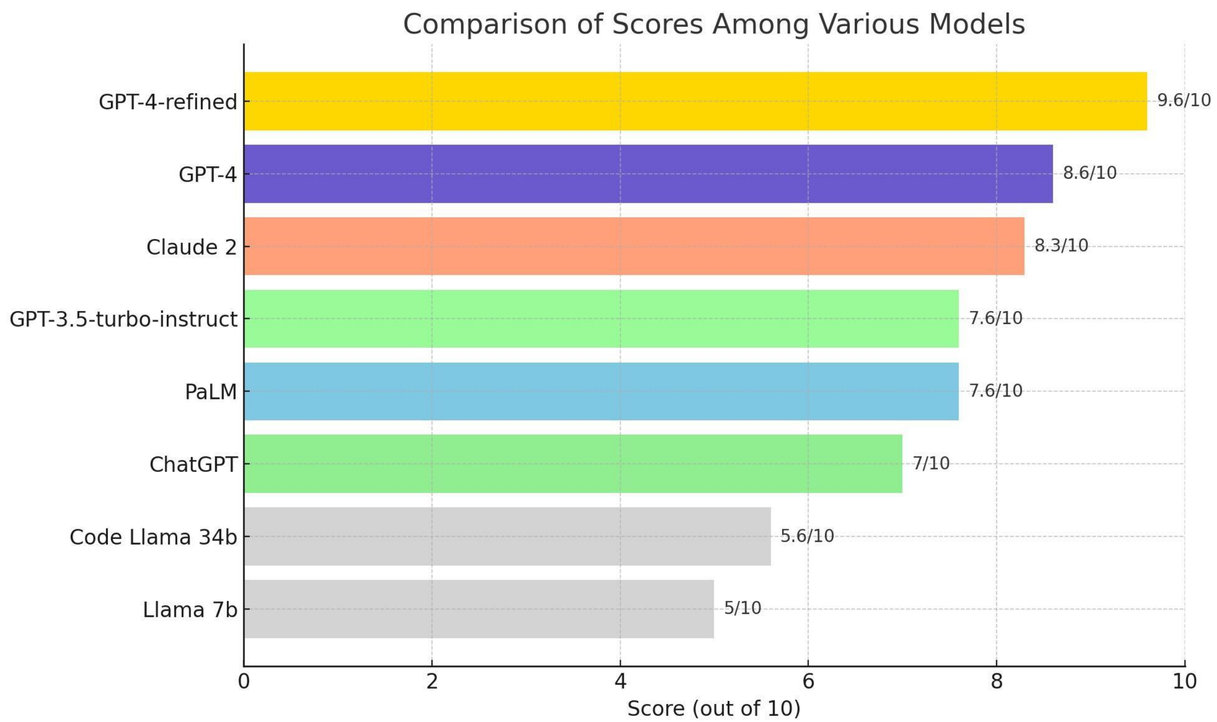
LLM Model Comparison

Model Size and Customisation

Detection using Open-Source vehicle dataset

Training of Text based Model using CRISKLE data

Integration in CRISKLE



OpenAI – Customisation possible using Open AI platform.

LLAMA – customisation not possible in the cloud. Provides Generic output

CLAUDE – customisation not possible in the cloud. Provides Generic output

GEMINI – customisation not possible in the cloud. Provides Generic output

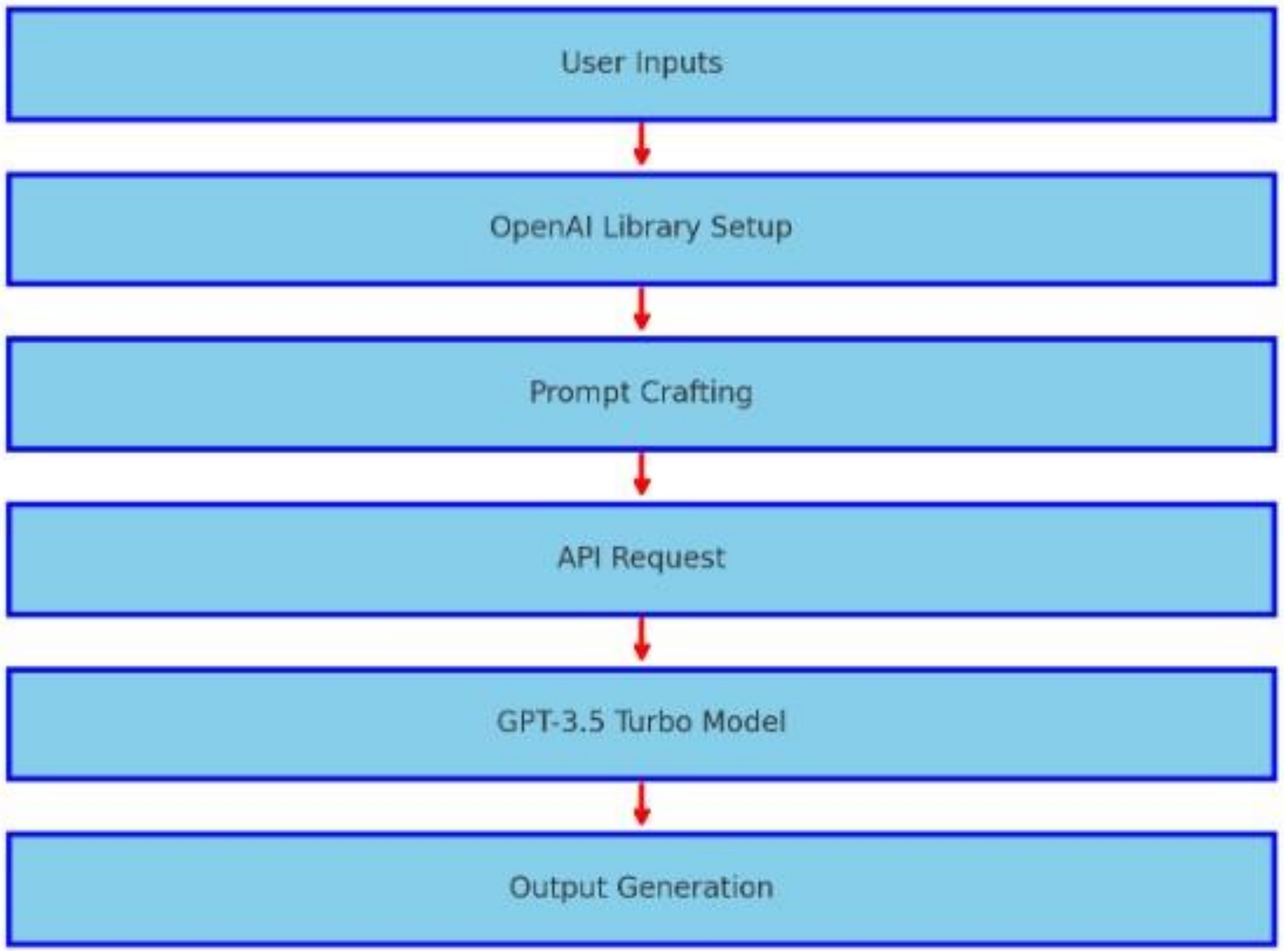
Model Training – Trial 2

LLM Example : OpenAI - Threat Scenario Generation

Detection using Open-Source vehicle dataset

Training of Text based Model using CRISKLE data

Integration in CRISKLE



Model Training

Threat Scenario Generation

Detection using Open-Source vehicle dataset

↓

Training of Text based Model using CRISKLE data

↓

Integration in CRISKLE

10 Generated Threat Scenario

A hacker gains access to a vehicle's CAN bus and exploits a vulnerability in the infotainment system, allowing them to remotely control the vehicle's functions and potentially steal sensitive personal information from the driver.
Malicious actor exploits a vulnerability in a vehicle's Bluetooth connectivity to gain remote access and control over critical systems, such as brakes and steering.
Malicious actor hacks into a vehicle's onboard computer system, gaining unauthorized access to control critical functions such as brakes, steering, and acceleration. The attacker may exploit vulnerabilities in the software or use soc
A hacker gains access to a vehicle's internal network and manipulates the CAN bus to send false signals, causing the vehicle's brakes to malfunction while in motion. The attacker exploits a vulnerability in the system's software to g
Hackers gain access to a vehicle's CAN bus and exploit a vulnerability in the infotainment system, allowing them to remotely control the vehicle's functions and steal sensitive data.
Cybercriminal hacks into a vehicle's infotainment system through a compromised Wi-Fi connection, allowing them to access sensitive data and control the vehicle's functions remotely.
A hacker gains access to a vehicle's CAN bus system and manipulates the data to spoof signals, causing the car to accelerate or brake unexpectedly, potentially causing a collision.
Malicious actor hacks into the vehicle's infotainment system through a remote code execution vulnerability, gaining control over critical functions such as braking and steering.
A cyber criminal hacks into the vehicle's CAN bus system and gains control of the brakes, causing them to malfunction and potentially leading to a dangerous accident. The attacker exploits a vulnerability in the vehicle's software to
A hacker exploits a vulnerability in a vehicle's remote access system to gain control of the car's functions, including acceleration and braking, causing a potentially dangerous situation for the driver and passengers.

Output :

- Complete Threat scenario
- System based Contextualised output

Model Architecture

Threat Scenario Confirmation as Listed in Annex 5

Detection using Open-Source vehicle dataset

↓

Training of Text based Model using CRISKLE data

↓

Integration in CRISKLE

Annex 5

List of threats and corresponding mitigations

1. This annex consists of three parts. Part A of this annex describes the baseline for threats, vulnerabilities and attack methods. Part B of this annex describes mitigations to the threats which are intended for vehicle types. Part C describes mitigations to the threats which are intended for areas outside of vehicles, e.g. on IT backends.
2. Part A, Part B, and Part C shall be considered for risk assessment and mitigations to be implemented by vehicle manufacturers.
3. The high-level vulnerability and its corresponding examples have been indexed in Part A. The same indexing has been referenced in the tables in Parts B and C to link each of the attack/vulnerability with a list of corresponding mitigation measures.
4. The threat analysis shall also consider possible attack impacts. These may help ascertain the severity of a risk and identify additional risks. Possible attack impacts may include:
   (a) Safe operation of vehicle affected;
   (b) Vehicle functions stop working;
   (c) Software modified, performance altered;
   (d) Software altered but no operational effects;
   (e) Data integrity breach;
   (f) Data confidentiality breach;
   (g) Loss of data availability;
   (h) Other, including criminality.

Part A. Vulnerability or attack method related to the threats

Generated Threats compared to Threats listed in R155 Annex 5

```
# print results
Similer= docs_new[0].page_content
print(docs_new[0].page_content) # most similar
```

```
Manipulation of electronic hardware, e.g. unauthorized electronic hardware added to a
vehicle to enab le "man -in-the-middle" attack
```

Mitigation – Security Controls

Mitigation – Security Controls (R155 Annex 5)

Detection using Open-Source vehicle dataset

↓

Training of Text based Model using CRISKLE data

↓

Integration in CRISKLE

LLM Based Control Mechanism used for Security Control determination - Model

```
    # Check if the 'page_content' is contained by or contains the 'Threat_Description'
    #if query_content in threat_description or threat_description in query_content:
    if query_content in threat_description:
        # Print the corresponding mitigation measure
        print(f"Mitigation Measure: {row['Mitigation']}")
        match_found = True
        break  # Exit the loop after finding the first match

if not match_found:
    print("No matching threat description found in the CSV.")
    # After the loop, these prints would refer to the last row processed in the loop if no match is found
    # If you intend to print the last 'Threat_Description' processed and it didn't match, ensure correct indentation
```

```
Mitigation Measure: Measures to prevent and detect unauthorized access shall be employed
```

Integration of Model

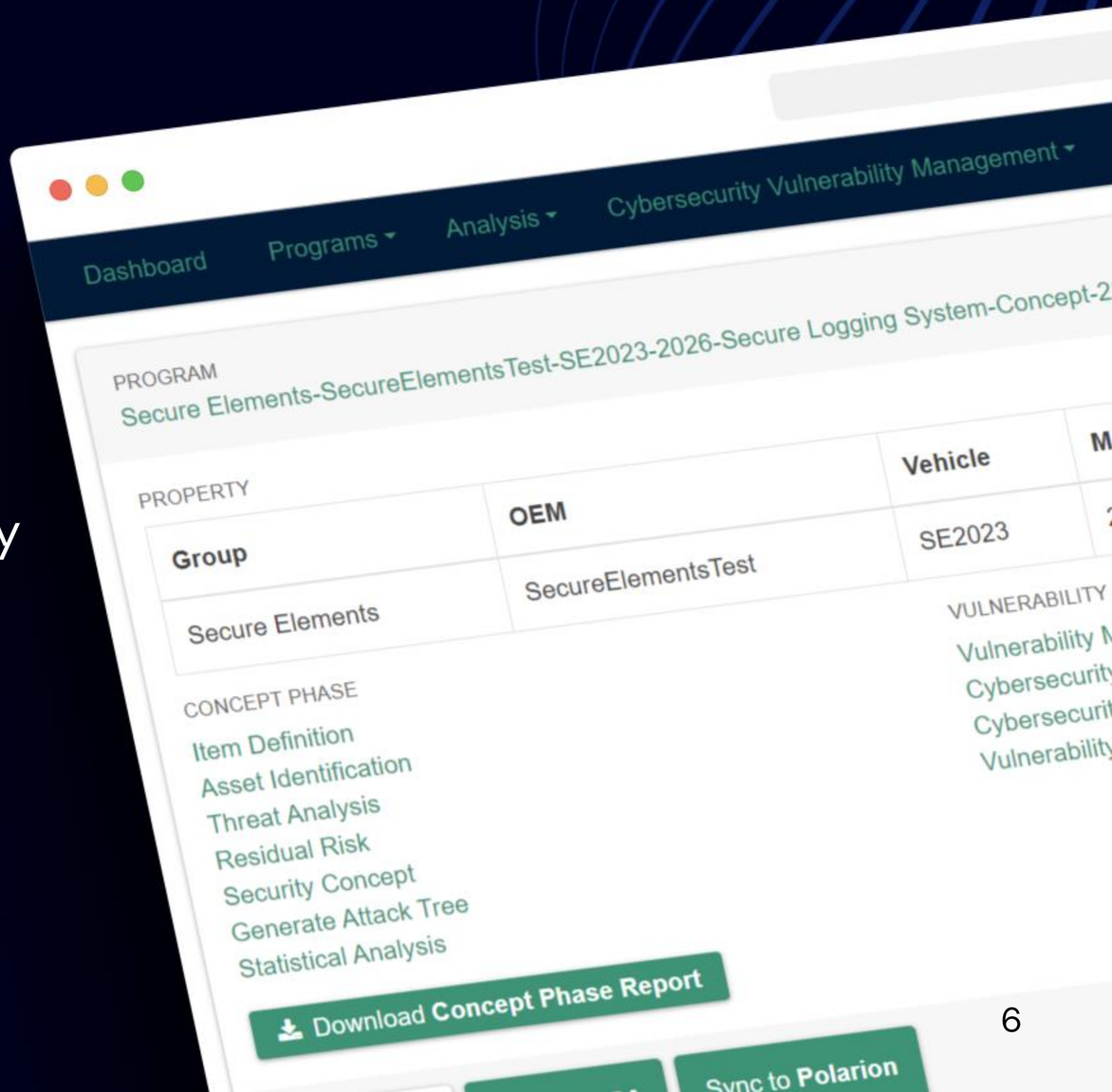
Product Cybersecurity Engineering Application

CRISKLE™

Integrates Systems, Safety and Cybersecurity Engineering Processes to assess

- Product Cybersecurity Risks and
- Cybersecurity Vulnerabilities

Through out the Product Lifecycle



Application Integration

Model Integration in CRISKLE

Detection using Open-Source vehicle dataset

↓

Training of Text based Model using CRISKLE data

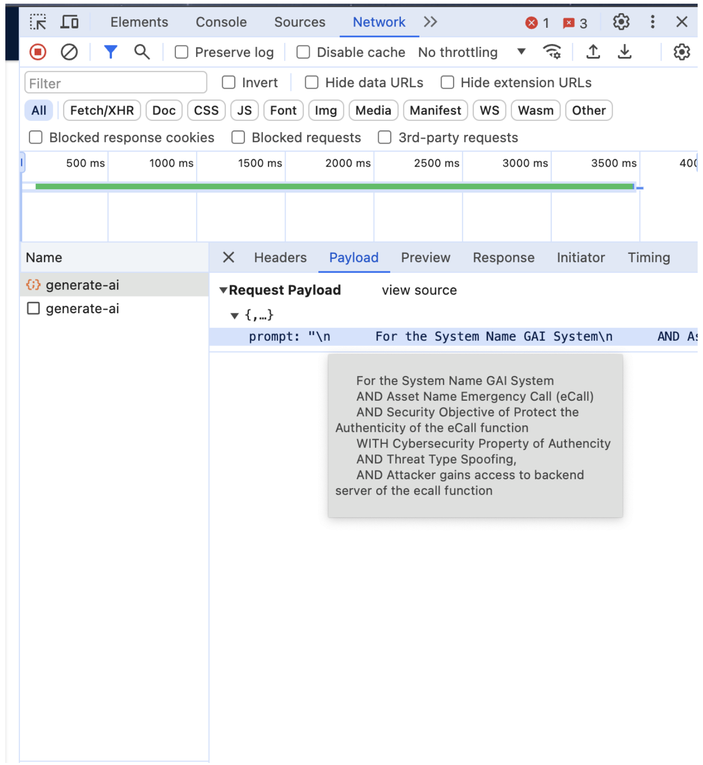
↓

Integration in CRISKLE

Inputs to the Threat Scenario Model

LLM generated Threat Scenario in CRISKLE, where, system Inputs are provided using templates : Default Template {

•System Name
•Asset Name
•Security Goal/Objective
•Cybersecurity Property
•Is threat type part of WP29 Annex. 5:
•Define Threat Sub-scenario:
•Threat Type: Spoofing
•Threat Scenario text (User Input) }



==========

Example scenario generation template:

{

- For the System Name Connected and Automated System
- AND Asset Name CANSignalName
- AND Security Objective of Protect the Authenticity of the CAN Signal
- WITH Cybersecurity Property of Authenticity
- AND is part of WP29 of Threats related to Vehicle Communication Channel
- WITH this Threat sub-scenario Loss of vehicle data and code
- AND Threat Type Spoofing
- AND Threat Scenario Description Attacker gains access to in vehicle CAN communication bus via remote access

}

Application

Integration in CRISKLE TARA

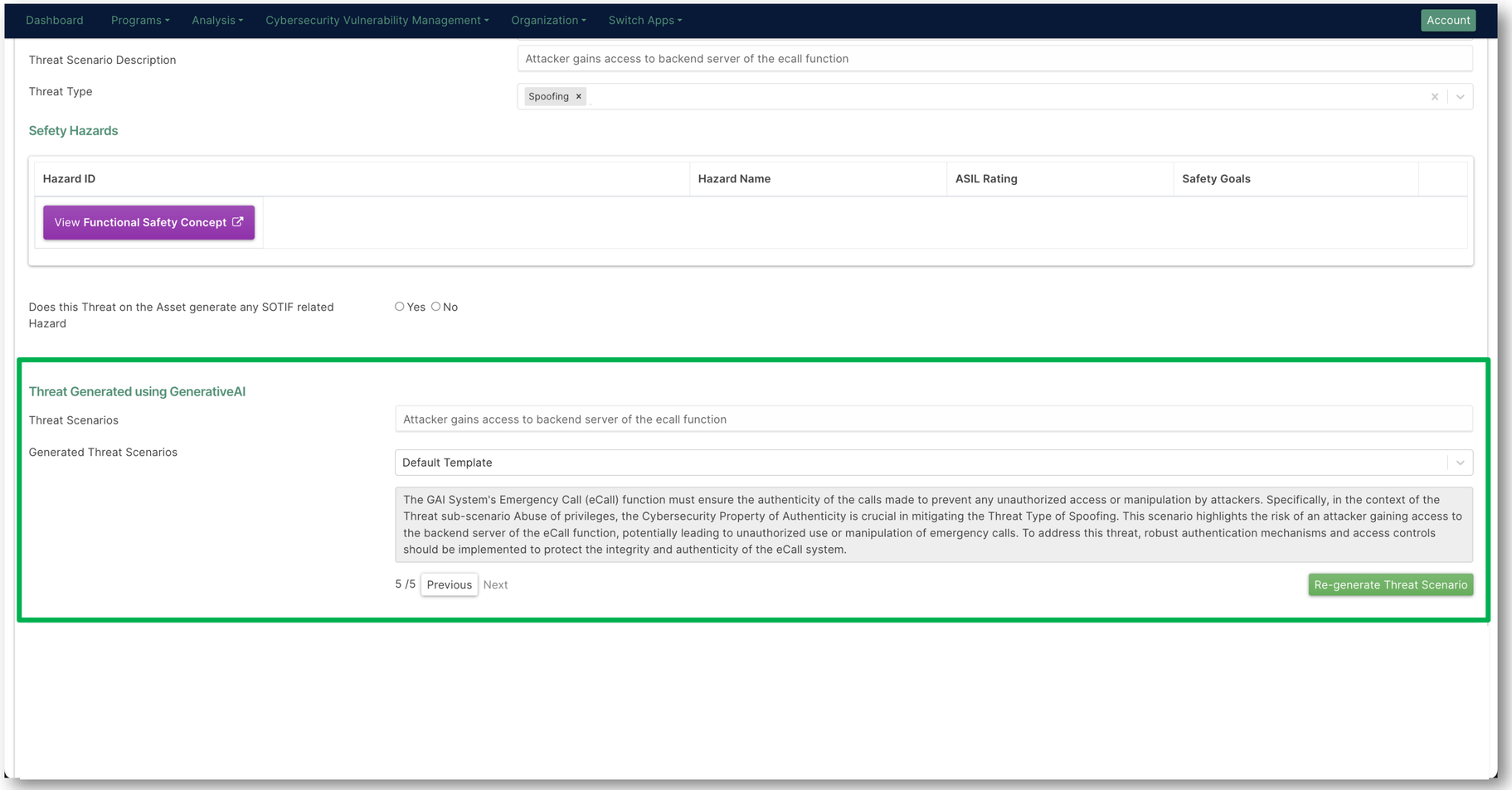
Detection using Open-Source vehicle dataset

↓

Training of Text based Model using CRISKLE data

↓

Integration in CRISKLE



Conclusion

It is possible to generate quality threat scenarios and mitigation controls for cybersecurity assessments by leveraging LLM's.

~~Excel Based TARA Tools for Threat Modelling~~

GenAI Based TARA Tools

~~Lack of experienced personnel to conduct TARA Assessments~~

AI/LLM based TARA can assist engineers to complete TARA Assessments

~~Significant/continual human effort required to conduct TARA on >60 ECU's /Vehicle~~

Reduced labour/time/cost

Result

TARA becomes a ~~static~~ dynamic document

- ❖ Capability to generate/auto complete threat scenario/s
- ❖ Auto complete relationship between Threat Scenarios and Mitigations
- ❖ Reduces labor, increasing speed of performing TARA thereby increasing productivity.
- ❖ Steps beyond R155 and looks at wide areas of Attacks (subject to model training)

Challenges

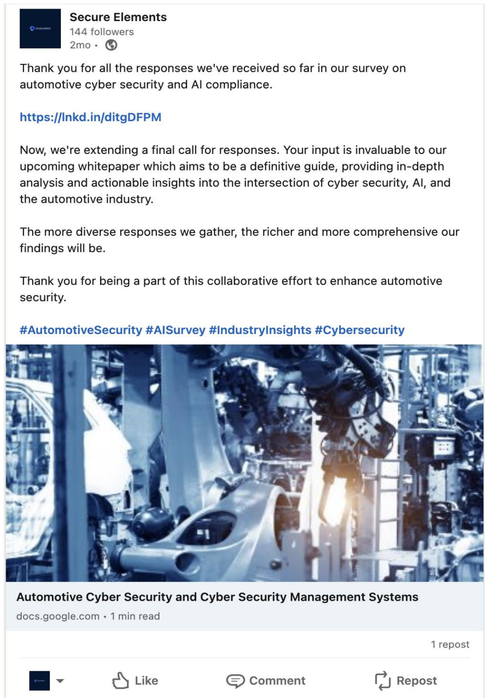
Key Challenges

- ❖Limited training data
- ❖Limited Time – 6 months [Challenging for Certifying and Annotating results]
- ❖GDPR/Privacy of data [confidentiality] was not part of project but must be thoroughly addressed.
- ❖Model training takes long time [HPU needed]
- ❖Careful selection of LLM algorithms.
- ❖Access to real vehicle data, DBC data and CAN Logs.

Project Achievements

Some of our achievements this quarter -

- Research Paper submitted for ITS World Congress 2024 - Accepted
- Attended the AESIN Plenary for Project Dissemination activity
- LinkedIn Campaign on acceptance of GenAI for Cybersecurity - Data being put together



SECURE ELEMENTS
INTEGRATING SECURE MOBILITY SOLUTIONS

Thank you

Interested in Trialing CRISKLE for Cybersecurity Risk Assessments to achieve UNECE R155 compliance ?

SCAN ME

Company Details

Registered at

Secure Elements Ltd.

Registered at

Union House 111 New Union Street Coventry
CV1 2NT United Kingdom
Company number 13876395

Contact Details

Mr. Saket Mohan
Email: saket.mohan@secureelements.co.uk

TechWorks AI

Launchpad

Bletchley Park
Milton Keynes

16th April 2024

Swansea University Prifysgol Abertawe

TechWorks

UKRI Innovate UK

BridgeAI

Panel Discussion