AI Security Test Engineer Intern [IDA: 00077]

Tvoji zadaci

Work Scope:
The intern will work on developing AI-powered automation tools to enhance security testing and validation activities across in automotive systems. The scope includes designing and implementing AI-based mechanisms to analyze system interfaces, security requirements, project artifacts, and standards, and to automatically generate test cases, test strategies, and technical reports. The intern will contribute to data preparation, automation workflows, and iterative validation to improve test coverage, reduce manual effort, and strengthen early detection of security and robustness issues using existing AI models.

Abstract / Description of the Project
This project aims to build an AI-driven interface fuzzing framework to identify hidden vulnerabilities, robustness gaps, and abnormal behavior in automotive ECUs and communication interfaces. The framework will use AI based models to learn protocol patterns directly from raw network traffic and AI agents to dynamically adjust fuzzing strategies based on system responses. This allows the tool to generate intelligent, context-aware fuzz inputs rather than relying on traditional random fuzzing.
During their tenure at Aumovio, the intern will be responsible for delivering the following work packages:

Work Package1: Support AI Based Fuzzing activity
The intern will support the development of the AI-Based Interface Fuzzing Framework by preparing and organizing interface traffic data, assisting in building preprocessing scripts, and helping generate test input templates for the fuzzing workflow. They will contribute to setting up test environments, running fuzzing sessions, monitoring system responses, and documenting anomalies or unexpected behaviors. Additionally, the intern will assist in refining the fuzzing strategy based on feedback from system behavior and help maintain the automation and testing infrastructure to ensure smooth execution of the AI-driven fuzzing process.

Work Package 2: AI-based Tooling to Generate Testcases from Security Requirements and identify missing Test cases from STDL
The intern will be responsible for designing and developing the AI-based model for generating security-focused test cases using Aumovio's existing AI capabilities. Extending testing beyond functional validation is essential because:

- Functional tests only verify expected behavior, whereas attackers target abnormal, adversarial, and unexpected conditions that lie outside normal workflows.

ID posla
REF6148B

Sektor
Inženjering

Lokacija
Singapore

Pravno lice
AUMOVIO Singapore Pte. Ltd.

- Many security vulnerabilities emerge in edge cases, error handling paths, and unintended feature interactions, requiring threat-based and robustness testing.
- Modern automotive security standards (ISO 21434, CRA, RED-DA) mandate resilience and adversarial validation, making non-functional security testing critical for compliance.

The intern will be responsible for the following (but not limited to):

1. Training existing AI models using available security test scenarios, automotive cybersecurity standards (ISO 21434, RED-DA, CRA, etc.), and emerging technology requirements to enable intelligent test case generation from security requirements and also identify the missing test scenarios from the existing ones in STDL.
2. Preparing and structuring datasets, building preprocessing pipelines, and designing prompt or data-driven mechanisms that allow the model to produce missing, high-value, or specification-aligned security test scenarios.
3. Conducting iterative experimentation for training, evaluating, and refining the model; validating generated test cases; and ensuring alignment with STDL structure, logic, and regulatory expectations.
4. Developing automation workflows to evaluate model outputs, documenting methodologies and results, and continuously tuning the model to improve detection of interface failures and cybersecurity weaknesses—ultimately enhancing overall test coverage and reducing manual authoring effort.

Work Package 3: AI Powered Report Generation Tool

The intern will be responsible for designing and developing the AI-powered report generation tool, ensuring that raw data from logs, test results, or system outputs is transformed into clear, accurate, and context-aware reports. The intern will also contribute to automation, validation, and documentation to ensure the tool delivers reliable and consistent outputs.

The intern will be responsible for the following (but not limited to):

1. Analyze reporting requirements, source data, and relevant documentation to define report structure and key metrics.
2. Collect, clean, and organize datasets to enable effective AI-driven report generation.
3. Build preprocessing pipelines to standardize and structure data for model input.
4. Train the existing AI models in Aumovio to generate automated reports from raw data.
5. Iteratively test and refine the model to improve clarity, accuracy, and relevance of outputs.
6. Validate generated reports against expected outputs and compliance standards.
7. Implement automation workflows for streamlined report generation.
8. Document development processes, model design, and methodologies for maintenance and future enhancements.

Work Package 4: Generation of Project specific SP Test Strategy using AI

The intern will be responsible to build an AI/LLM-based automation engine that generates customized Security & Privacy (SP) Test Strategies for individual projects. This involves using AI models to interpret project artifacts—such as system requirements, architecture details, TARA

outputs, standards, and customer-specific SP checklists—and converting them into a structured, project-aligned SP testing approach.

Key Responsibilities:
- Analyze inputs such as project requirements, system architecture, TARA, and relevant standards/customer SP checklists.
- Use LLMs/NLP techniques to extract key security elements and map them to SP testing areas.
- Apply the generic SP test strategy template to structure AI-generated outputs for each project.
- Assist in designing rules, prompts, or data pipelines that help the AI model adapt strategies to different project types.
- Validate model-generated SP strategies with sample projects and refine logic for accuracy and completeness.
- Support workflow automation to streamline generation, review, and documentation steps.

Tvoj profil

- Currently pursuing Bachelor's degree in Computer Science, Information Technology, or any other engineering stream with interest in software development, AI/ML, or cybersecurity.
- Coursework or academic exposure in AI/ML, data structures & algorithms, software testing, or cybersecurity is highly advantageous.
- Candidates with prior projects or experience in machine learning, automation, scripting, or security-focused assignments will be strongly preferred.

Core Qualifications:

Naša ponuda

Ready to take your career to the next level? The future of mobility isn't just anyone's job. Make it yours! **Join AUMOVIO. Own What's Next.**

O nama

Since its spin-off in September 2025 AUMOVIO continues the business of the former Continental group sector Automotive as an independent company. The technology and electronics company offers a wide-ranging portfolio that makes mobility safe, exciting, connected, and autonomous. This includes sensor solutions, displays, braking and comfort systems as well as comprehensive expertise in software, architecture platforms, and assistance systems for software-defined vehicles. In the fiscal year 2024 the business areas, which now belong to AUMOVIO, generated sales of 19.6 billion Euro. The company is headquartered in Frankfurt, Germany and has about 87.000 employees in more than 100 locations worldwide.