netidee

PROJEKTE

MONITAUR

Zwischenbericht | Call 18 | Projekt ID 6872

Inhalt

1 Einleitung

Dieser Bericht beschreibt die im Rahmen des Projekts bis Ende Dezember 2024 geleistete Arbeiten. Der Fokus im Berichtszeitraum lag auf der Erhebung und Konsolidierung der Anforderungen an unser Toolkit (Arbeitspaket 2), der Recherche und Untersuchung aktueller Überwachungsmethoden, und der Entwicklung des Toolkits (Arbeitspaket 3). Außerdem haben wir in Vorbereitung auf die Integration in Open-Source-Überwachungstools die zu exportierenden Metriken und Warnhinweise für die Endnutzer definiert (Arbeitspaket 4). Der Fortschritt jedes einzelnen Arbeitspakets wird im Kapitel 2 im Detail beschrieben.

Alle Arbeitspakete verlaufen nach Plan. Allerdings mussten wir einen größeren Teil der Arbeit in die zweite Hälfte des Projekts verschieben, da wir in Arbeitspaket 3 eine unerwartet große Anzahl von Methoden zu berücksichtigen hatten, auf die wir in Kapitel 2.3 näher eingehen. Diese Verschiebung führte zu einer verspäteten Halbzeitberichterstattung. Der ursprünglich geplante Zeitplan für die Blogbeiträge ist davon ebenfalls betroffen; wir werden dies kompensieren, indem wir in den letzten Monaten des Projekts mehr Einträge veröffentlichen.

2 Status der Arbeitspakete

2.1 Arbeitspaket 1 - Detailplanung und Formales am Projektstart

Mit dem Abschluss dieses Arbeitspakets mit Ende Februar 2024 haben wir alle formalen Anforderungen zu Beginn des Projekts erfüllt. Wir haben einen detaillierten Projektplan erstellt, den ersten Projektblog veröffentlicht und den Antrag auf die erste Finanzierungsrate gestellt. Das Arbeitspaket wurde wie geplant abgeschlossen.

2.2 Arbeitspaket 2 - Requirements and landscape analysis

Der Fokus von Arbeitspaket 2 war die Ermittlung der Anforderungen für unser Projekt. Zunächst waren Interviews mit Experten aus der Industrie, die entweder Überwachungslösungen entwickeln oder potenzielle Nutzer von MONITAUR sein würden, geplant, um realistische Anforderungen für unser System zu erhalten. Leider erwiesen sich Details zu solchen Lösungen als äußerst vertraulich, und wir konnten keine Experten rekrutieren. Daher änderten wir den Ansatz, und fokussierten uns auf akademische Studien, die die Erfahrungen und das Interesse von Industriepraktikern an den Sicherheitsbedrohungen des maschinellen Lernens untersuchten, einschließlich der Angriffe durch Modelldiebstahl, die MONITAUR entschärfen soll. Wir veröffentlichten unseren zweiten Blog auf der Grundlage dieser Studien und nutzten sie, um die Anforderungen für MONITAUR zu formulieren. Obwohl wir den Fokusändern mussten, wurde das Arbeitspaket wie geplant bis Ende April 2024 abgeschlossen.

2.3 Arbeitspaket 3 - Collection and development of monitoring methods

Dieses Arbeitspaket widmet sich dem Bewerten und Implementieren von Überwachungsmethoden. Zu Beginn des Arbeitspakets stellten wir fest, dass die Anzahl der

veröffentlichten Methoden zur Erkennung verdächtiger Clients stark gestiegen war – im Vergleich zu unserer ersten Untersuchung im Juli 2023 hatte sich die Zahl der Methoden verdreifacht (von 10 auf 30). Da wir uns mit allen Methoden vertraut machen wollten, nahm die erste Phase der Methodensammlung mehr Zeit in Anspruch als erwartet, und es folgte ein zeitaufwendiger Prozess der Eingrenzung der Kandidatenliste. Deswegen verschoben wir den Start der Methodenentwicklung, was zu einer Verlagerung des Arbeitsaufwandes in die zweite Hälfte des Projekts führte. Dadurch waren auch die Blogbeiträge verzögert, was wir durch vermehrte Beiträge in den kommenden Monaten kompensieren werden.
Zum Berichtszeitpunkt ist das Arbeitspaket abgeschlossen. Wir haben ein einheitliches Rahmenwerk für Überwachungsmethoden entwickelt und vier Überwachungsmethoden implementiert. Das Arbeitspaket wurde wie geplant bis Ende Dezember 2024 abgeschlossen.

2.4 Arbeitspaket 4 - Monitoring Cockpit, Integration of Detectors, Testing and Deployment

In diesem Arbeitspaket erfolgt die Integration unseres Toolkits in Open-Source Überwachungssysteme. Bis Ende Dezember2024 hatten wir potenzielle Kandidaten für die Integration unseres Toolkits gesammelt, Metriken definiert, die an die Endnutzer kommuniziert werden müssen, und Warnregeln festgelegt. Wir begannen daraufhin den Integrationsprozess mit Prometheus[1]. Für den Rest des Arbeitspakets planen wir, mehrere andere Überwachungssysteme zu testen und uns dann auf die Visualisierung auf der Endbenutzerseite zu konzentrieren. Da dieses Arbeitspaket von Arbeitspaket 3 abhängt, wurde auch hier ein Teil des Arbeitspensums in die zweite Projekthälfte verlagert. Wir erwarten jedoch keine Verzögerungen und planen, dieses Arbeitspaket wie geplant bis Ende März 2025 abzuschließen.

2.5 Arbeitspaket 5 - Dokumentation und Formales am Projektende

Dieses Arbeitspaket wird Anfang Februar 2025 anlaufen.

3 Umsetzung Förderauflagen

Das Projekt hat keine speziellen Förderauflagen.

4 Zusammenfassung Planaktualisierung

Aufgrund der Verschiebung der Tätigkeiten wurde die Berichterstattung zur Projektmitte von August auf Dezember verschoben. Der Zeitplan für die Arbeitspakete bleibt unverändert.

5 Öffentlichkeitsarbeit/ Vernetzung

[1] https://prometheus.io/

Im Rahmen des Arbeitspakets 2 haben wir mit einigen Branchenvertretern gesprochen, die daran interessiert sein könnten, entweder ihr Produkt mit unserer Lösung zu erweitern oder unsere Lösung zum Schutz ihrer Dienste einzusetzen. Wir werden sie erneut kontaktieren, wenn die Entwicklung von MONITAUR abgeschlossen ist. Darüber hinaus planen wir, MONITAUR in weiteren Forschungsprojekten einzusetzen und darüber zu publizieren, um es in der Forschungsgemeinschaft zu verbreiten.

6 Eigene Projektwebsite

Der Code, die Dokumentation und die Empfehlungen werden auf GitHub veröffentlicht. Eine zusätzliche Website ist nicht geplant.