HÖHERE TECHNISCHE BUNDESLEHRANSTALT Wien 3 Rennweg
Höhere Abteilung für Mechatronik
Höhere Abteilung für Informationstechnologie
Fachschule für Informationstechnik

Antrag um Genehmigung einer Aufgabenstellung für die

Diplomarbeit

2025/26	**3R IT 26 02**
Schuljahr	Projektnummer (durch AV vergeben)

VulnTURE – F57 Security & Alert Tooling

Projektthema (Arbeitstitel)

Das Projekt **VulnTURE** entwickelt eine zentrale Plattform zur automatisierten Sammlung, Analyse und Korrelation sicherheitsrelevanter Informationen. Sicherheitsfeeds wie jene von CERTs oder Herstellerwarnungen werden regelmäßig abgerufen und mit einer Asset-Datenbank abgeglichen, um Bedrohungen wie Sicherheitslücken oder DDoS-Angriffe frühzeitig erkennen zu können. Erkennt das System eine Übereinstimmung, werden Hinweise gespeichert und gezielte Warnungen an verantwortliche Personen versendet. Zentrale Funktionen sind eine Asset-Verwaltung mit CRUD, ein Benachrichtigungssystem, ein Rollen- und Rechtemodell, Protokollierung sowie ein Analysemodul zur DDoS-Erkennung.

Aufgabenstellung

Projektteam

Schülerin/Schüler	Klasse	Individuelle Betreuung	Unterschrift
David Grübling Projektleiter:in/Product Owner	5AI	WAG	Projektleiter:in/Product Owner
David Franz Stellv. Projektleiter:in/Scrum Master	5AI	BAY	Stellv. Projektleiter:in/Scrum Master
Max Hackenberg Projektmitarbeiter:in	5AI	WAG	Unterschrift Projektmitarbeiter:in

Projektbetreuung:

Matthias Wagner Individuelle Betreuung (Hauptbetreuung)	Unterschrift Hauptbetreuer:in
Mitra Bayandor Individuelle Betreuung (Hauptbetreuung Stellv.)	Unterschrift Stellv. Hauptbetreuer:in

Als Diplomarbeit zugelassen am

AV Christian Schöndorfer

Inhaltsverzeichnis

1. Projektidee

1.1. Ausgangssituation

Das Projekt „VulnTURE“ entstand aus der Notwendigkeit, sicherheitsrelevante Informationen aus verschiedenen Quellen zu sammeln und diese mit eigenen oder betreuten Assets abzugleichen. Ziel ist es, Bedrohungen wie Sicherheitslücken oder DDoS-Angriffe schnell zu identifizieren und betroffene Systeme rechtzeitig zu warnen.
Das Projekt wird im Auftrag der Wiener Linien GmbH & Co KG umgesetzt.
Durch persönlichen Kontakt zu einem Mitarbeiter der Wiener Linien und in weiterer Folge zu einem IT-Verantwortlichen wurde die Idee konkretisiert und schließlich als Diplomarbeit vergeben. Die Wiener Linien beabsichtigen, das System nach Abschluss produktiv für die interne IT-Sicherheit einzusetzen, insbesondere zur Auswertung externer Sicherheitsmeldungen in Verbindung mit ihrer eigenen Asset-Infrastruktur.

Rahmenbedingungen des Projekts sind:

- Die Systemarchitektur basiert auf einem JavaScript-Stack mit Vue.js im Frontend, Node.js im Backend und MySQL als relationaler Datenbank auf einem Linux-Server.
- Die Anwendung umfasst Funktionen wie das Abrufen und Parsen von Sicherheitsfeeds, ein CRUD-basiertes Asset-Management, die Protokollierung von DDoS-Indikatoren sowie ein Warn- und Benachrichtigungssystem per E-Mail.
- Das Projekt wird in einer serverseitigen Umgebung betrieben.

1.2. Beschreibung der Idee

Das Projekt „VulnTURE“ verfolgt die Idee, eine zentrale Plattform zur automatisierten Beschaffung, Analyse und Korrelation sicherheitsrelevanter Informationen zu entwickeln.
Ziel ist es, Bedrohungen wie Sicherheitslücken oder DDoS-Angriffe frühzeitig zu erkennen und mit bestehenden Assets in Verbindung zu bringen. Durch das regelmäßige Abrufen von Daten aus verschiedenen Sicherheitsfeeds (z. B. CERTs, Herstellerwarnungen) werden potenzielle Gefahrenquellen identifiziert und automatisiert mit einer strukturierten Asset-Datenbank abgeglichen. Wenn ein Feed-Eintrag mit einem vorhandenen Asset in Zusammenhang gebracht werden kann, wird im System ein entsprechender Hinweis gespeichert. Basierend auf diesen Hinweisen können gezielt Warnungen über ein Web-Interface erstellt werden, die per E-Mail an verantwortliche Kontaktpersonen weitergeleitet werden. Mittels Vergleich stellt das System sicher, dass auch leicht abweichende, aber relevante Informationen zuverlässig erkannt werden.

Die Plattform umfasst folgende zentrale Komponenten:

- Eine Verwaltungsschnittstelle für Assets mit vollständiger CRUD-Funktionalität
- Ein Warn- und Benachrichtigungssystem zur manuellen Erstellung und Versendung von E-Mail-Warnungen
- Ein Benutzer- und Rollenkonzept zur geregelten Rechtevergabe und Zugriffskontrolle
- Protokollierungs- und Prüfmechanismen
- Ein Analysemodul zur Erkennung potenzieller DDoS-Ziele auf Basis externer JSON-Daten

2. Projektziele

Neben den Produktzielen werden während des Prozesses der Diplpomarbeit noch weitere Ergebnisse vom Team geliefert (z.B. Diplomarbeitsbuch, Projektmanagement-Dokumente, TOFT-Vorbereitung…).

2.1. Hauptziele

Das gesamte System, bestehend aus den unten angeführten Zielen, wird mit allen Kernfunktionen umgesetzt. Die gesamte Anwendung wird gemäß WCAG 2.1 (Konformitätsstufe AA) barrierefrei bis 17. März umgesetzt.

Ziel-H 1 FeedData Fetching

Ein Modul zum regelmäßigen Abrufen sicherheitsrelevanter Feeds ist implementiert, um die Grundlage für weitere Analysen zu schaffen.

Ziel-H 2 Feed Parsing

Die abgerufenen Feed-Daten werden verarbeitet und in strukturierter Form (siehe Ziel-H 4) weiterverwendbar abgelegt in der Datenbank abgelegt.

Ziel-H 3 Duplikat Erkennung

Es ist ein Verfahren zur zuverlässigen Erkennung und zum Ausschluss von doppelten Feed-Einträgen implementiert.

Ziel-H 4 Feed-Datenbankstruktur

Die Feed-Daten werden in einer relationalen Datenbank mit den Feldern Titel, Quelle, Typ, Schweregrad, Zeitstempel und Prüfsumme gespeichert.

Ziel-H 5 Benutzer und Rollenkonzepte

Es wird ein einheitliches Rollenkonzept entworfen, das klar definierte Benutzerrollen sowie deren Berechtigungen beschreibt.

Ziel-H 6 Asset anlegen

Administratoren können neue Asset-Datensätze im System erfassen.

Ein **Asset** ist ein zu schützendes System – dies kann sowohl Hardware (z. B. Server, Router, Arbeitsplatzrechner) als auch Software (z. B. Anwendungen, Datenbanken, Betriebssysteme) sein. Erfasst werden dabei Titel, Kontaktperson, Kategorie und aktueller Status des Assets.

Ziel-H 7 Asset bearbeiten

Administratoren können bestehende Asset-Datensätze über das Interface bearbeiten und aktualisieren.

Ziel-H 8 Asset löschen

Administratoren können nicht mehr benötigte Assets über das Interface dauerhaft löschen.

Ziel-H 9 Asset anzeigen & suchen

Im Interface wird eine tabellarische Übersicht mit Such- und Filterfunktionen für alle Assets bereitgestellt.

Ziel-H 10 CSV-Import Assets

Mehrere Assets können über eine CSV-Datei ins System geladen und automatisiert validiert werden.

Ziel-H 11 CSV-Validierung

Der Import prüft automatisch auf fehlende Felder oder falsche Formate und meldet diese zurück.

Ziel-H 12 Asset-Kategorien anlegen

Benutzer können Kategorien zur Gliederung von Assets erstellen und verwalten, um eine übersichtliche Struktur zu gewährleisten

Ziel-H 13 Kategorien deaktivieren

Benutzer können Kategorien zur Gliederung von Assets erstellen und verwalten. Nicht mehr benötigte Kategorien können deaktiviert werden, sodass sie für neue Zuordnungen nicht mehr verfügbar sind, bei bestehenden Assets jedoch zur Sicherung von Konsistenz und Nachvollziehbarkeit erhalten bleiben.

Ziel-H 14 Kategorien löschen

Das System erlaubt das Löschen einer Kategorie nur dann, wenn sie mit keinem Asset verknüpft ist, sodass die Datenbank jederzeit konsistent bleibt und keine fehlerhaften Beziehungen entstehen.

Ziel-H 15 DDoSIA Feed Analyse

Das System analysiert Feeds aus externen Quellen auf von DDoS betroffene Systeme.

Ziel-H 16 DDoSIA Musterprüfung

Die Feeds können mithilfe von Suchmustern gefiltert werden.

Ziel-H 17 DDoS-Zieldaten speichern

Informationen wie IP, URL, Port und SSL-Status von betroffenen Systemen werden strukturiert in der Datenbank gespeichert.

Ziel-H 18 Match-Speicherung

Alle erkannten Übereinstimmungen zwischen Feed und Asset werden in einer eigenen DB-Tabelle gespeichert.

Ziel-H 19 Warnung erstellen (manuell)

a. Benutzer können im System manuell neue Warnungen erstellen, wobei zwischen zwei Typen unterschieden wird: allgemeine Warnungen (ohne Bezug zu einem Asset) und assetbasierte Warnungen, bei denen relevante Asset-Daten wie Titel, Kategorie und Kontakt automatisch in das Formular übernommen werden.
b. Benutzer wählen eine passende Warnkategorie wie "alert" oder "ddos-alert" im Formular aus.
c. Der Benutzer trägt Betreff und Empfängeradressen manuell im Warnformular ein.

Ziel-H 20 Warntext automatisch befüllen

Das Warnformular füllt sich automatisch mit Informationen aus dem Feed- und Asset-Datensatz.

Ziel-H 21 Warnung per Mail versenden

Nach dem Speichern wird die Warnung per SMTP-E-Mail an die definierten Empfänger verschickt.

Ziel-H 22 E-Mail Retry & Logging

Ein Retry-Mechanismus sorgt für zuverlässige Zustellung and die ausgewählten Personen und Fehlerprotokollierung.

Ziel-H 23 System Logging

Das System protokolliert Ereignisse, Fehler und Benutzeraktionen zentral in Log-Dateien.

Ziel-H 24 Automatisierte Jira Ticketerstellung

Das System erstellt bei jeder neuen Warnung automatisch ein Jira-Ticket, das alle relevanten Informationen enthält und so eine zuverlässige Nachverfolgung der Meldungen ermöglicht.

2.2. Optionale Ziele

Ziel-O 1 Benutzerverwaltung

Benutzerkonten können angelegt, bearbeitet, deaktiviert und Gruppen zugewiesen werden.

Ziel-O 2 Gruppenrechte

Zugriffsrechte werden über Rollen und Gruppenzugehörigkeiten verwaltet.

Ziel-O 3 Login & Authentication System

Ein Login-System mit sicherer Benutzer-Authentifizierung wird optional integriert.

Ziel-O 4 Zwei-Faktor-Authentifizierung (MFA)

Ein optionales MFA-System wird zur zusätzlichen Zugriffssicherung implementiert.

Ziel-O 5 Feedquellen verwalten

Administratoren können neue Feeds über ein Interface hinzufügen oder bearbeiten.

Ziel-O 6 Interface-Verbesserung

Das UI wird bei Gelegenheit anhand von Testuserfeedback während der Entwicklung weiterentwickelt.

Ziel-O 7 Sicherheits-Updates

Technische Komponenten und Bibliotheken werden regelmäßig sicherheitsseitig aktualisiert.

Ziel-O 8 Fuzzy Matching

Ein Fuzzy-Algorithmus erkennt ähnliche Begriffe mit einer konfigurierbaren Ähnlichkeitsschwelle.

Ziel-O 9 Substring Matching

Das System vergleicht Feed- und Asset-Namen auf direkte Übereinstimmung über Teilzeichenketten.

Ziel-O 10 TOFT-Präsenz

Am Tag der Offenen Tür unserer Schule, am 7. und 8. November 2025 und dem 24. Jänner 2026, wird unsere Diplomarbeit präsentiert, um Interessierte über unser Projekt zu informieren.

a. Ein Plakat zum Aushängen in dem Gang ist nach Vorlagen der Schule erstellt und ausgedruckt worden.
b. Ein Stand ist geplant ebenso wird ein weiteres kreatives Plakat erstellt.
c. Alle notwendigen Werbematerialien, wie etwa Visitenkarten, ein QR-Code sowie Bildschirme für die Präsentation und die Vorführung des Prototypen, sind vorhanden.

2.3. NICHT-Ziele

Ziel-N 1 Mobile App

Das System wird als Mobile App umgesetzt.

Ziel-N 2 KI-Funktionen

Es werden KI- oder ML-Modelle für Matching oder Analyse eingesetzt.

Ziel-N 3 Automatischen Gegenmaßnahmen

Das System reagiert automatisch auf Bedrohungen, sondern informiert nicht nur.

Ziel-N 4 Multi-Tenancy

Das System unterstützt gleichzeitige Nutzung durch mehrere Organisationen.

Ziel-N 5 öffentliche API

Es werden externe Programmierschnittstellen zur Verfügung gestellt.

Ziel-N 6 Zahlungsfunktionen

Das Projekt enthält Bezahl- oder Lizenzlogik.

Ziel-N 7 Mobile Optimierung

Das Interface wird speziell für Smartphones oder Tablets angepasst da der Hauptverwendungszweck kleine Bildschirme sind.

Ziel-N 8 Cloud-native Infrastruktur

Das System wird cloudbasiert oder mit automatischer Skalierung betrieben.

Ziel-N 9 Schulungsinhalte

Es wird Schulungssystem oder Benutzerhilfe erstellt.

2.4. Individuelle Aufgabenstellungen der Teammitglieder im Projekt

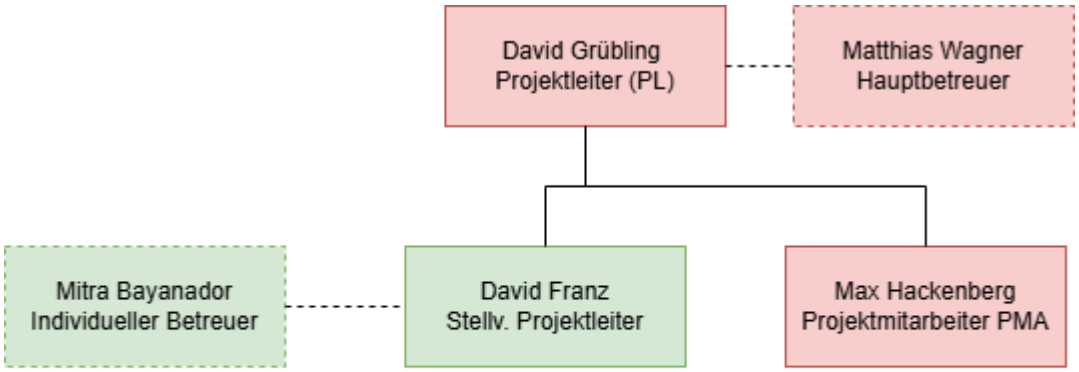
David Grübling	**Projektleiter:in**
David Grübling führt als Projektleiter den Kundenkontakt und übernimmt die Rolle des Product Owners. Seine Aufgaben umfassen das Implementieren der Feed-Verarbeitung (Abruf, Parsing, Duplikat-Erkennung, Datenbankstruktur), die Speicherung von Matches sowie den Versand und das Logging von Warnungen per E-Mail.	
» ZIEL-H 1 FeedData Fetching » ZIEL-H 2 Feed Parsing » ZIEL-H 3 Duplikat Erkennung (Checksum) » ZIEL-H 4 Feed-Datenbankstruktur » ZIEL-H 18 Match-Speicherung » Ziel-H 21 Warnung per Mail versenden » Ziel-H 22 E-Mail Retry & Logging » Ziel-O 1 Benutzerverwaltung » Ziel-O 2 Gruppenrechte » Ziel-O 3 Login & Authentication System » Ziel-O 6 Interface-Verbesserung » Ziel-O 10a TOFT-Präsenz	

David Franz	**Stellv. Projektleiter:in**
David Franz ist als Scrum Master für den reibungslosen Ablauf des Projekts auf Management-Ebene verantwortlich. Darüber hinaus entwickelt er zentrale Funktionen im Frontend und Backend, insbesondere die Verwaltung von Assets und Kategorien, das manuelle Erstellen von Warnungen sowie die automatisierte Erstellung von Jira-Tickets.	
» ZIEL-H 6 Asset anlegen » ZIEL-H 7 Asset bearbeiten » ZIEL-H 8 Asset löschen » ZIEL-H 9 Asset anzeigen & suchen » Ziel-H 12 Asset-Kategorien anlegen » Ziel-H 13 Kategorien deaktivieren » Ziel-H 14 Kategorien löschen » ZIEL-H 19a Warnung erstellen (manuell) » ZIEL-H 19b Warnkategorie wählen » Ziel-H 24 Automatisierete Jira Ticketerstellung » ZIEL-O 4 Zwei-Faktor-Authentifizierung (MFA) » ZIEL-O 5 Feedquellen verwalten » ZIEL-O 7 Sicherheits-Updates » Ziel-O 10b TOFT-Präsenz	

Max Hackenberg	**Mitarbeiter:in**
Max Hackenberg entwickelt Funktionen im Frontend und Backend zur Verarbeitung sicherheitsrelevanter Datenquellen. Zu seinen Aufgaben zählen das Benutzer- und Rollenkonzept, der CSV-Import mit Validierung, die Analyse und Speicherung von DDoS-Daten, die Unterstützung beim Erstellen von Warnungen sowie das zentrale System-Logging.	
» ZIEL-H 5 Benutzer und Rollenkonzepte » ZIEL-H 10 CSV-Import Assets » ZIEL-H 11 CSV-Validierung » ZIEL-H 15 DDoSIA Feed Analyse » ZIEL-H 16 DDoSIA Musterprüfung » ZIEL-H 17 DDoS-Zieldaten speichern » ZIEL-H 19c Warnung: Betreff & Empfänger » ZIEL-H 20 Warntext automatisch befüllen » ZIEL-H 23 System Logging » ZIEL-O 8 Fuzzy Matching » ZIEL-O 9 Substring Matching » Ziel-O 10c TOFT-Präsenz	

3. Projektorganisation

3.1. Grafische Darstellung



Hauptbetreuer Matthias Wagner

Hauptbetreuer Stellvertreterin Mitra Bayandor

3.2. Projektteam

Funktion	Name	Kürzel	E-Mail
PL	David Grübling	GRÜ	1038@htl.rennweg.at
PL Stv.	David Franz	FRA	1037@htl.rennweg.at
PMA	Max Hackenberg	HAC	1039@htl.rennweg.at

4. Stakeholderanalyse

Nr. (Ext/Int)	Bezeichnung des Stakeholders (SH)	Beschreibung des Einflusses Wie kann der SH das Projekt ev. unterstützen, wie behindern?	Einfluss auf Projekt/Macht (gering/hoch)	Einstellung zum Projekt (positiv/negativ)	Maßnahmen
Int-01	Projektteam/Auftragnehmer (David Franz, David Grübling, Max Hackenberg)	Kennt Projektziele genau, kann flexibel arbeiten und schnell umsetzen. Mangelnde Motivation oder schlechte Zusammenarbeit kann den Fortschritt beeinträchtigen. Zeitdruck oder interne Konflikte können das Projekt auch gefährden.	hoch	positiv	- Daily Scrums - Scrum retrospective - Bei jedem Sprint-Planning soll auf die Fähigkeiten der Teammitglieder geschaut werden Aufgaben im Scrum Backlog klar aufteilen , indem wir eine Scrum Board benutzen.
Ext-01	Wiener Linien GmbH & Co KG (Auftraggeber)	Stellen Anforderungen, Budget oder Ressourcen bereit. Können Anforderungen kurzfristig ändern oder Projekt stoppen.	hoch	positiv	- Wenn die Kommunikation zwischen Projektteam und Auftraggeber*in klar genug ist, können Missverständnisse und somit auch Fehler vermieden werden: - Regelmäßige Meetings vereinbaren, um Informationen zu geben - Termine im Kalender beachten - Frühs möglichst Hindernisse klären und aus dem Weg schaffen (Meeting mit AG) - schriftliche Fixierung der Ergebnisse in Protokollen und E-Mails, damit alle Beteiligten dieselben Informationen haben und Missverständnisse vermieden werden
Int-02	Matthias Wagner (Hauptbetreuer)	Gibt wertvolles technisches Feedback und hilft bei Problemen. Kann bei Nichtverfügbarkeit oder falscher Richtung Verzögerungen verursachen.	hoch	positiv	- Regelmäßige Meetings - Offene Fragen früh klären - Absprachen klar dokumentieren - konsensuelle Entscheidungen treffen.
Int-03	Mitra Bayandor (Stellvertretende Betreuung)	Unterstützt bei Dokumentation und Bewertung. Kann zu viele Änderungen an der Projektstruktur verlangen.	hoch	positiv	- Regelmäßige Meetings - Offene Fragen früh klären - Absprachen klar dokumentieren - konsensuelle Entscheidungen treffen.
Ext-02	Wiener Linien Abteilung f57 (User)	Können wertvolles Feedback zur Nutzerfreundlichkeit liefern. Können das Tool ablehnen oder schlecht annehmen, wenn es nicht nutzerfreundlich ist.	hoch	positiv	- Testuser besorgen - Prototypen frühzeitig zeigen - Bekommenes Feedback einbauen

Ext-03	Paul Hoffmann (Ansprechpartner Wiener Linie)	Unterstützt als direkter Kontakt, vermittelt intern, gibt Feedback. Kann Informationen verzögert weiterleiten oder Anforderungen missverständlich übermitteln.	Hoch	Positiv	- Regelmäßige Meetings - Einladen zu Sprint Reviews - Feedback aktiv einholen
Ext-03	Lukas Spannbruckner (Ansprechpartner Wiener Linien)	Unterstützt als direkter Kontakt, vermittelt intern, gibt Feedback. Kann Informationen verzögert weiterleiten oder Anforderungen missverständlich übermitteln.	Hoch	Positiv	- Regelmäßige Meetings - Einladen zu Sprint Reviews - Feedback aktiv einholen

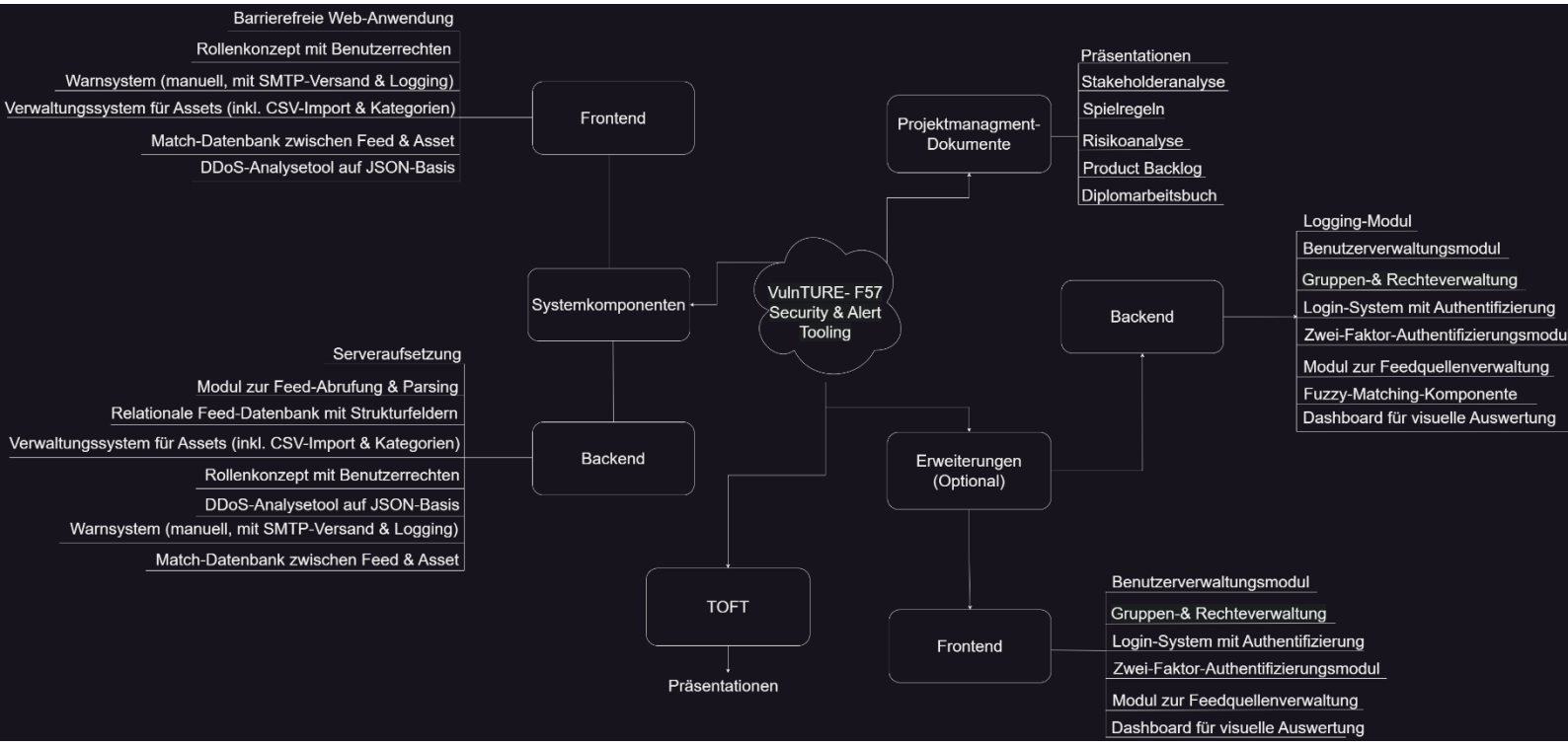
4.1. Stakeholder Portfolio

Einfluss/Macht: viel / wenig

Zufriedenstellen Int-01 Projektteam/Auftragnehmer Ext-01 Wiener Linien GmbH & Co KG Ext-02 Wiener Linien Abteilung f57	Eng managen (hoher Aufwand) Int-01 Projektteam/Auftragnehmer Int-02 Mitra Bayandor Int-03 Matthias Wagner Ext-03 Paul Hoffmann Ext-04 Lukas Spannbruckner
Überwachen (wenig Aufwand betreiben)	Informieren/auf dem Laufenden halten Int-02 Matthias Wagner Int-03 Mitra Bayandor Ext-03 Paul Hoffmann Ext-04 Lukas Spannbruckner

− Einstellung zum Projekt +

5. Objektstrukturplan/Betrachtungsobjekteplan



6. Backlog

Siehe Backlog im Anhang A.

7. Risikoanalyse

7.1. Risikotabelle

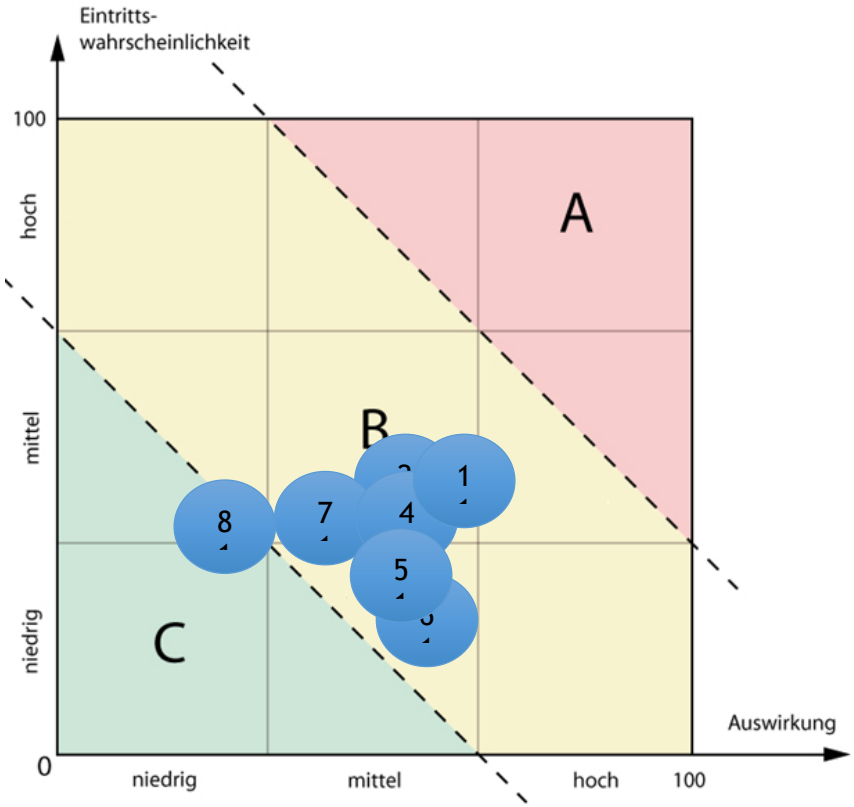
	RISIKO		AUSWIRKUNG				MASSNAHMEN	
#	Bezeichnung	Beschreibung	P	A	RF	Verzögerung (in Wochen)	… zur Reduktion v. P bzw. A[1] oder für den Fall des Risikoeintritts einen Plan B überlegen	Kosten
1	Fehlendes Fachwissen	Mangelndes Fachwissen führt zu Verzögerungen im Projektablauf, wodurch vereinbarte Deadlines nicht eingehalten werden können.	50	75	3750	5	Bei auftretenden Wissenslücken werden unsere Ansprechpartner hinzugezogen oder externe Ressourcen genutzt. Dadurch wird sichergestellt, dass Aufgaben ohne größere Verzögerungen umgesetzt werden können	_
2	Schlechtes Zeitmanagement	Deadlines werden übersehen, wodurch sich das Projekt verzögert, und der geplante Starttermin gefährdet ist.	50	70	3500	5	Durch die Scrum-Meetings ist jedem Teammitglied bewusst, welche Aufgaben jeweils innerhalb dieses Sprints zu erledigen sind. Ebenso werden Deadlines im Kalender eingetragen	-
3	Konflikte innerhalb des Teams	Innerhalb des Projektteams könnten Streitigkeiten, Meinungsverschiedenheiten oder unklare Zuständigkeiten entstehen, was zu Verzögerungen im Projekt führt.	40	60	2400	2	Die Aufgabenverteilung erfolgt transparent und werden in Protokollen festgehalten, indem jedes Teammitglied seine Aufgaben eigenständig und rechtzeitig erledigt, um Missverständnisse zu vermeiden. Durch das Daily Scrum Meeting werden die Aufgaben besprochen, um Probleme zu vermeiden	-
4	Falsche Daten	Die ins System importierten sicherheitsrelevanten Feed-Daten könnten fehlerhaft, unvollständig oder manipuliert sein. Dadurch könnten falsche Analysen, irreführende Warnungen oder eine unzureichende Risikoeinschätzung entstehen.	45	50	2250	3	Es wird eine Validierung der Feed-Daten beim Import implementiert. Zusätzlich werden Feedquellen dokumentiert und klassifiziert, um ihre Vertrauenswürdigkeit bewerten zu können. Optional kann ein manueller	-

							Prüfprozess für kritische Daten aktiviert werden, diese werden mit dem externen Partner besprochen werden.	
6	Unzureichende Benutzerfreundlichkeit	Die App ist zu kompliziert oder komplex gestaltet, sodass Schüler*innen sie nicht gerne nutzen.	30	60	1800	3	Die App wird mit Minimalistischen und intuitives Design umgesetzt, um die Benutzerexperience und Benutzerfreundlichkeit zu bieten. User Test werden mit der Usern aus der Zielgruppe durchgeführt.	-
7	Krankheiten und Ausfälle bei wichtigen Terminen	Durch Krankheit oder unerwartete Ausfälle können zentrale Termine nicht wie geplant stattfinden. Das führt zu Verzögerungen oder Qualitätsverlusten.	30	60	1800	1	Präsentationsunterlagen frühzeitig fertigstellen und zentral ablegen; laufende Dokumentation sicherstellen, damit im Notfall ein anderes Teammitglied übernehmen kann; wichtige Termine nach Möglichkeit hybrid durchführen.	-
8	Performanceprobleme bei großen Datenmengen	Bei sehr vielen Feeds oder Assets kommt es zu langen Ladezeiten, langsamer Duplikaterkennung oder verzögerter Warnungserstellung.	40	30	1200	3	Datenbank-Indizes optimieren, Serverlast überwachen, ggf. Archivierung implementieren.	-

P...Eintrittswahrscheinlichkeit des Risikos , A...Schadensausmaß bei Eintritt des Risikos , RF...berechneter Risikofaktor

[1] Maßnahmen zur Risikovermeidung oder -verringerung überlegen oder Risikoabwälzung bzw. Risikoakzeptanz (Restrisiko). Kosten für die Risikomaßnahmen nicht vergessen.

7.2. Risikoportfolio



8. Meilensteinliste

#	Meilenstein	SOLL-Termin	IST-Termin
1	Fertigstellung der Planung	15.Sep.2025	-
2	Einrichtung der Entwicklungsumgebung abgeschlossen	15.Sep.2025	-
3	Einreichung der Diplomarbeit in der DA Datenbank abgeschlossen	29.Sep.2025	-
4	UI für die Seiten für TOFT fertiggestellt	07.Nov.2025	
5	Fertigstellung der Kernfunktionen	20.Nov.2025	-
6	Interne Präsentation abgeschlossen	25.Nov.2025	-
7	Erweiterung & Optimierung der UI abgeschlossen	20.Dez.2025	
8	Erste Version der schriftlichen Diplomarbeit fertiggestellt	09.Feb.2026	-
9	Entgültige Implementierung abgeschlossen	1.März.2026	
10	Abnahme und Endpräsentation durchgeführt	17.März.2026	-

9. Projektressourcen

9.1. Projektressourcen: Soll - Ist Vergleich

SOLL Bereich	IST	Risiko-Nr.	User-story Num-mer
Infrastruktur für Testumgebung (Docker)	vorhanden	1	85
Know How über die DDoS Quellen	nicht ausreichend	2	55, 57
Zugang zu aktuellen Sicherheitsfeeds	nicht vorhanden	3	45
Know How im Bereich Incident Response	nicht ausreichend	4	63
Rechtliche / Compliance Expertise (DSGVO, BSI, WCAG)	teilweise vorhanden	5	
Know How Monitoring und Logging	teilweise vorhanden	6	42
Know How zur Erstellung & Automatisie-rung von Jira-Tickets bei Warnungen	Ist nicht vorhanden	7	123

9.2. Personelle Ressourcen

#	Teammitglied	Personenstunden
1	David Grübling	170
2	David Franz	160
3	Max Hackenberg	160
SUMME		490

9.3. Erwartete Kosten für die Durchführung des Projektes

Pos.	Bezeichnung des Aufwands	Kosten
	Gesamtkosten	€ 0

9.4. Kostendeckung

Für dieses Projekt fallen keine Kosten an.

10. Geplante externe Kooperationspartner

Wiener Linien GmbH & Co KG
Art der Kooperation: Die Wiener Linien bzw. die Abteilung F57 - Nachrichtentechnik und Zugsicherung treten als offizieller Auftraggeber des Projektes auf. Im Rahmen der Diplomarbeit wird ein neues, eigenständiges Sicherheits- und Warnsystem entwickelt, das externe Feeds automatisiert analysiert und mit einer gepflegten Asset-Datenbank abgleicht. Die Wiener Linien stellen fachliche Anforderungen bereit, beraten bei sicherheitsrelevanten Themen und unterstützen die Evaluierung der Ergebnisse.

10.1. Sponsoren

Für dieses Projekt gibt es keine Sponsoren.

11. Geplante Verwertung der Ergebnisse

Das entwickelte Interface wird den Wiener Linien nach Abschluss der Diplomarbeit offiziell übergeben und soll anschließend im täglichen Betrieb zur automatisierten Sicherheitsüberwachung und Warnung eingesetzt werden. Die Wiener Linien planen, das System produktiv zu nutzen, um externe Sicherheitsmeldungen effizient auszuwerten und interne Schutzmaßnahmen schneller einleiten zu können.

Der Quellcode verbleibt zusätzlich als GitHub-Repository Klon von der Wiener Linien bei der Projektgruppe. Den Wiener Linien wird ein uneingeschränktes nicht exklusives Nutzungsrecht des Programmcodes vom Stand der Übergabe eingeräumt.

Eine verbindliche Festlegung kann nach gemeinsamer Abstimmung mit allen Projektbeteiligten sowie nach einer rechtlichen Klärung angepasst oder geändert werden.

Anhang A

[VUL-42] Als System möchte ich sicherheitsrelevante Feeds regelmäßig abrufen, damit eine Grundlage für Analysen geschaffen wird.
[VUL-43] Als System möchte ich Feed-Daten strukturieren und in der Datenbank speichern, damit sie weiterverwendbar sind.
[VUL-44] Als System möchte ich doppelte Feed-Einträge erkennen und ausschließen, damit keine redundanten Informationen gespeichert werden.
[VUL-45] Als Entwickler möchte ich die Feed-Daten in einer relationalen Datenbank mit spezifischen Feldern ablegen, damit sie effizient analysiert werden können.
[VUL-46] Als Administrator möchte ich ein Rollenkonzept mit klar definierten Berechtigungen nutzen, damit Benutzer nur auf autorisierte Funktionen zugreifen.
[VUL-47] Als Administrator möchte ich neue Assets anlegen können, damit ich zu schützende Systeme dokumentieren kann.
[VUL-48] Als Administrator möchte ich bestehende Assets bearbeiten können, damit ihre Informationen aktuell bleiben.
[VUL-49] Als Administrator möchte ich nicht mehr benötigte Assets löschen können, damit das System übersichtlich bleibt.
[VUL-50] Als Benutzer möchte ich alle Assets in einer Tabelle sehen und filtern können, damit ich gezielt suchen kann.
[VUL-51] Als Administrator möchte ich mehrere Assets per CSV importieren können, damit ich effizient große Datenmengen hinzufügen kann.
[VUL-52] Als System möchte ich CSV-Daten beim Import validieren, damit fehlerhafte Datensätze erkannt und zurückgemeldet werden.
[VUL-53] Als Benutzer möchte ich Kategorien für Assets anlegen, damit ich sie thematisch gruppieren kann.
[VUL-54] Als Benutzer möchte ich nicht mehr genutzte Kategorien deaktivieren können, damit bestehende Daten erhalten bleiben, aber neue nicht fehlerhaft kategorisiert werden.
[VUL-55] Als System möchte ich externe Feeds auf DDoS-Betroffenheit analysieren, damit Risiken erkannt werden.
[VUL-56] Als Analyst möchte ich Feeds mit Suchmustern filtern können, um gezielt relevante Informationen zu extrahieren.
[VUL-57] Als System möchte ich DDoS-Zieldaten wie IP, Port und SSL-Status speichern, um betroffene Systeme zu dokumentieren.
[VUL-58] Als System möchte ich Matches zwischen Feeds und Assets speichern, um potenzielle Gefährdungen sichtbar zu machen.
[VUL-59] Als Benutzer möchte ich manuell neue Warnungen erstellen können, um auf Vorfälle aufmerksam zu machen.
[VUL-60] Als Benutzer möchte ich eine Warnkategorie auswählen, um die Art der Warnung zu definieren.
[VUL-61] Als Benutzer möchte ich Betreff und Empfänger einer Warnung selbst eintragen, um gezielt Personen zu informieren.
[VUL-62] Als System möchte ich das Warnformular automatisch mit Feed- und Asset-Daten befüllen, um manuelle Eingaben zu reduzieren.
[VUL-63] Als System möchte ich Warnungen per E-Mail an definierte Empfänger senden, damit wichtige Informationen schnell verteilt werden.
[VUL-64] Als System möchte ich bei E-Mail-Versand Wiederholungsversuche und Fehlerprotokollierung durchführen, um eine zuverlässige Zustellung sicherzustellen.

[VUL-65] Als System möchte ich Ereignisse, Fehler und Benutzeraktionen zentral protokollieren, damit Transparenz und Nachvollziehbarkeit gewährleistet sind.
[VUL-66] Als Administrator möchte ich Benutzerkonten verwalten können, damit ich Nutzer effizient organisieren kann.
[VUL-67] Als Administrator möchte ich Zugriffsrechte über Gruppen und Rollen steuern, damit die Berechtigungen zentral verwaltbar sind.
[VUL-68] Als Benutzer möchte ich mich über ein sicheres Login-System anmelden können, damit nur autorisierte Personen Zugriff erhalten.
[VUL-69] Als Benutzer möchte ich eine Zwei-Faktor-Authentifizierung nutzen, damit mein Zugang zusätzlich gesichert ist.
[VUL-70] Als Administrator möchte ich Feedquellen verwalten, damit ich neue Feeds hinzufügen oder bearbeiten kann.
[VUL-71] Als Entwickler möchte ich das Interface anhand von Nutzerfeedback verbessern, damit die Bedienbarkeit steigt.
[VUL-72] Als System möchte ich regelmäßig Sicherheitsupdates erhalten, damit bekannte Schwachstellen geschlossen werden.
[VUL-73] Als System möchte ich ähnliche Begriffe über Fuzzy Matching erkennen, damit auch unscharfe Treffer erfasst werden.
[VUL-74] Als System möchte ich Asset- und Feednamen per Substring-Matching vergleichen, damit ich einfache Teiltreffer erkennen kann.
[VUL-85] Als Entwickler möchte ich eine Entwicklungsumgebung mit Docker aufsetzen, um das Projekt lokal laufen zu lassen.
[VUL-121] Als Projektteam möchten wir eine Website erstellen, auf der wir unser Team vorstellen, damit Besucher einen Überblick über die Teammitglieder, deren Rollen und unsere gemeinsame Diplomarbeit erhalten.
[VUL-122] Als Benutzer möchte ich Kategorien löschen können, jedoch nur dann, wenn diese Kategorie nicht bei einem Asset verwendet wird, damit Datenkonsistenz gewährleistet bleibt und keine fehlerhaften Verknüpfungen entstehen.
[VUL-123] Als System möchte ich, dass automatisch ein Jira-Ticket erstellt wird, sobald eine neue Warnung im System erfasst wird, damit diese Meldung direkt im Projektmanagement-Tool nachverfolgt und priorisiert werden kann.