MTEP idėjos tikrinimo ataskaita

Projekto idėja: DI technologijomis paremtos, gebančios atlikti automatinę įmonės dokumentacijos atitikties patikrą bei pateikti atitikčiai užtikrinti reikalingas rekomendacijas, pagal pasirinktą saugos standartą, programinės įrangos modelio kūrimas.

Finansavimo programa: Lietuvos Respublikos švietimo, mokslo ir sporto ministerijos mokslo plėtros programa, pažangos priemonė Nr. 12-001-01-02-01

Projekto autorius: MB "AG Cyber"

Projekto vadovas: Antanas Kedys

Projekto trukmė: 2024-12-01 iki 2025-05-31

Ataskaitos data: 2025–06-13

Turinys

Finansuoja Europos Sąjunga NextGenerationEU

Įžanga

Šis projektas buvo skirtas išbandyti dirbtiniu intelektu (toliau – DI) sudarytu iš RAG (retrieval-augmented generation) ir LLM (large language model) paremto programinės įrangos modelio galimybes automatiškai tikrinti organizacijos dokumentaciją pagal antrąją Tinklų ir informacinių sistemų saugumo (TIS2) direktyvą (Toliau – NIS2) ir galinio vartotojo (toliau - Naudotojo) laisva forma įvestus atsakymus į pateiktus klausimus iš NIS2 direktyvos, apdoroti šią informaciją ir pateikti atitikties NIS2 direktyvai statusą ir konkrečias rekomendacijas skirtas atitikties trūkumams pašalinti ir įvertinus įkeltą dokumentaciją ir įvestus atsakymų į klausimus užtikrinti atitiktį NIS2 direktyvai. Šio projekto metu sukurta programinė įranga toliau ataskaitoje toliau vadinama pavadinimu

“ComplAInce”. Nors projekto pradiniuose planuose buvo paminėta, jog bus naudojamas GPT-3 arba GPT-4 LLM bei RPA - tačiau projektavimo fazėje, pasitelkus ekspertų (DI ir programuotojų) žinias bei atsižvelgiant į projekto architektūra buvo nuspręsta, vietoje GPT-3 ir GPT-4 naudoti LLAMA 70B arba GROK2 (dėl tikslesnio modelio pritaikomumo sprendimui, geresnės integracijos, kokybės bei kainos), o RPA atsisakyti dėl nereikalingos atskiros automatizacijos dalies šio projekto apimtyje, bei galimybės darbus automatizuoti ir įgyvendinti su DI įskaitant RAG ir FAISS vektorinę paieškos sistemą, nenaudojant papildomų sprendimų, kurie nepridėtų vertės galutiniam “ComplAInce” produktui.

Projektas buvo įgyvendintas ruošiantis dalyvavimui programoje “Europos horizontas“. Šioje ataskaitoje pateikiami galutiniai “MB AG Cyber” įgyvendinto MTEP projekto rezultatai, įskaitant testavimus, rinkos analizę, bei nuorodas į sukurtą DI modelį (prototipą), pilno “ComplAInce” programinės įrangos vizualinį sprendimą.

Tikslai ir uždaviniai

- Išbandyti “ComplAInce” technologines galimybes, identifikuoti, problemas bei patikrinti rinkos realizacijos potencialą ir realaus praktinio panaudojimo galimybę.
- Įvertinti RAG ir DI modelius, jų privalumus, trūkumus, taikymą ir tikslumą.
- Sukurti prototipą, leidžiantį automatiškai analizuoti dokumentus ir Naudotojo atsakymus bei pateikti atitikties NIS2 vertinimą su rekomendacijomis atitikčiai užtikrinti.
- Sukurti ir ištestuoti demonstracinę vartotojo sąsają prototipui, kuri būtų funkciškai veikianti.
- Sukurti vizualinį “ComplAInce” dizaino prototipą, įvertinus galimų Naudotojų suteiktą informaciją, testavimo rezultatus, kuris būtų patrauklus Naudotojui ir pateiktu vizualinę informaciją, kaip turėtų atrodyti užbaigta “ComplAInce” programinė įranga, po šio projekto sėkmingai dalyvaujama projekte “Europos horizontas”.
- Surinkti rinkos ir technologinės analizės duomenis, juos įvertinti ir pritaikyti prototipui.
- Pasirengti dalyvavimui “Europos horizontas“ kvietimuose.

Metodologija, pagrindiniai metodai ir atlikti darbai

Projektas buvo vykdomos vadovaujantis prototipo kūrimo, technologinio tinkamumo įvertinimo (proof-of-concept), interviu ir eksperimentinio vertinimo principais bei metodais.

Pagrindiniai atlikti darbai su “ComplAInce” DI dalimi:

- Didelio masto kalbos modelio (LLM) LLAMA 70B diegimas dokumentų analizės procese. Modelis buvo naudojamas analizuoti naudotojo atsakymus ir įkeltus dokumentus pagal NIS2 atitikties reikalavimus.
- Alternatyvių LLM modelių testavimas, siekiant palyginti atsakymų tikslumą, generavimo laiką ir atitikties interpretavimo galimybes.
- RAG (retrieval-augmented generation) architektūros taikymas, siekiant pagerinti modelio gebėjimą generuoti atsakymus remiantis informacija iš Naudotojo įkeltų dokumentų bei iš pačiame “ComplAInce” ikeltų NIS2 dokumentų. Tokiu būdu buvo siekiama maksimaliai išvengti „hallucination” (neteisingų) tipo atsakymų ir užtikrinta kokybė.
- Vektorinės duomenų bazės (embedding + semantinė paieška) naudojimas teksto ir informacijos paieškai pagal semantinę prasmę, o ne tikslias frazes. Šis metodas leido surasti susijusius dokumento fragmentus net esant skirtingoms formuluotėms ir Naudotojo laisvai įrašytam tekstui o ne tiesiogiai kaip parašyta NIS2.
- Dokumentų skaidymas į semantinius segmentus, jų klasifikavimas pagal atitikimo politikos tipus (informacijos saugumo politika, incidentu planas ir kt.). Tokia struktūra leido taikyti analizę taškiniu būdu, padidinant tikslumą ir sumažinant „false positive“ riziką.
- Modelio testavimas su realiais atvejais, siekiant įvertinti modelio ribas ir atsparumą neapibrėžtoms, dviprasmėms ar netipinėms formuluotėms,kurios naudojamos realiame pasaulyje ir realiose įmonėse, taip pat buvo analizuotas rekomendacijų nuoseklumas bei jų vertė Naudotojui.

Pagrindiniai atlikti darbai su “ComplAInce” ne DI dalimi (dizainas, Naudotojo patrities (UX/UI)):

- Prototipo testavimas su tiksliniais Naudotojais, surenkant grįžtamąjį ryšį apie sąsajos aiškumą ir patogumą.
- Naudotojo kelio (user flow) analizė – nuo dokumentų įkėlimo, atsakymo į pateiktus klausimus įrašymo iki galutinės ataskaitos ir rekomendacijų peržiūros.
- Rekomendacijų aiškumo testavimas – siekiama įvertinti ar Naudotojas be papildomos pagalbos supranta, ką reikia daryti visos patirties (Nuo “ComplAInce” pirminio lango iki ataskaitos lango) metu, kiekviename žingsnyje.
- “ComplAInce” dizainas sukurtas ateities plėtrai ir galutiniam produkto įgyvendinimui su “Europos horizontas“ programa, optimizuotas mobiliesiems įrenginiams ir didesniems duomenų kiekiams, informacijai bei platesnėms situacijoms.

Vykdant projektą buvo sukurtas pilnai vekiantis prototipas, skirtas tiek demonstraciniam naudojimui, tiek būsimos pilnos platformos plėtrai. Pagrindiniai prototipo aspektai ir atlikti darbai:

- Prototipo programavimas - Įgyvendintas šiuolaikiškas, interaktyvus vartotojo sąsajos dizainas, pritaikytas net ir techninių žinių neturinčiam naudotojui bei integruotas su sukurtu DI modeliu, įgyvendintos saugumo priemonės ir prieigos valdymas.
- Frontend – naudota Angular.
- Backend – naudota Spring Boot, Kotlin, PostgreSQL .
- Išorės prieigai ir apsaugai nuo kibernetinių atakų – Cloudflare.
- Naudojama modulinė architektūra, leidžianti lengvai plėtoti funkcionalumą ateityje.
- Realizuotos pagrindinės funkcijos: dokumentų įkėlimas, klausimyno pildymas, analizės paleidimas, ataskaitos ir rekomendacijų peržiūra.

Naudoti ištekliai

Projekto įgyvendinimui buvo pasitelkti įvairūs ištekliai – tiek žmogiškieji, tiek techniniai ir išoriniai. Atsižvelgiant į projekto pobūdį (R&D), buvo suformuota maža, bet efektyvi specialistų komanda, kuri realizavo tiek dirbtinio intelekto komponentus, tiek IT, tiek vartotojo sąsajos bei prototipo sukūrimą. Techniniai sprendimai buvo realizuoti debesijos infrastruktūroje. Projekto metu buvo siekiama užmegzti tarptautinius ryšius ir rinkti rinkos įžvalgas dalyvavaujant pasaulinio lygio konferencijoje.

Žmogiškieji ištekliai:

- Projekto vadovas ir “MB AG Cyber” vadovas (*Antanas Kedys*):
  - Projekto vadovavimas ir strategija (techninė ir organizacinė)
  - Saugumo architektūra.
  - Sistemos veikimo architektūra.
  - Finansų valdymas.
  - Komandos valdymas ir resursų paskirstymas.
- DI programuotoja (*Monika Venčkauskaitė*):
  - DI modelio ir IT integracijos programavimas.
  - Skirtingų LLM ir DI testavimas ir optimalaus varianto parinkimas.
  - RAG testavimas.
  - Duomenų bazės sudarymas.
  - DI modelio pritaikymas pagal projekto vadovo pateiktą architektūrą.
  - API sąsajos sukūrimas.
- Frontend/backend programuotojas (*Rytis Stankus*):

  - Virtualios techninės aplinkos parengimas (Google Cloud, toliau - GCP).
  - Duomenų bazės optimizavimas.
  - Front-end prototipo programavimas ir integracija su back-end technine aplinka.
  - DI integracija į GCP Front-end ir Back-end.
  - Prototipo testavimas, programinio kodo klaidų taisymas.
- UI/UX dizaino ir Naudotojo patirties paslaugos (*MB Hait studio, Paulius Pipiras*):
  - UI/UX aplikacijos dizaino kūrimas.
  - Naudotojo sąsajos, patirties ir “ComplAInce” dizaino testavimas ir patogiausio varianto parinkimas.
  - Wireframes ir vizualinių prototipų sukūrimas (Figma).
  - Dizaino failų parengimas ir paruošimas programuotojams.

Techniniai ištekliai:

- Google Cloud Platform (CloudRun ir VMs) debesijos paslauga, įskaitant IAM funkcionalumą (Identity and access management).
- GitHub programinio kodo repozitorija.
- FAISS vektorinės paieškos sistema.
- LLAMA 70B LLM modelis (Groq).
- GROK2 LLM modelis.
- GROQ api - LLM api ir infrastruktūra.
- FIGMA platforma UX/UI darbams.
- Cloudflare prieigai iš išorės bei kibernetiniam saugumui.

Išoriniai ištekliai:

- Dalyvavimas RSA kibernetinio saugumo konferencijoje (San Franciskas), siekiant sužinoti apie DI panaudojimą bei pakalbėti su konkurentų ir panašių produktų atstovais apie problematikas ir DI sprendimo niuansus, rinką.
- Bandymai užmegzti ryšius su University of Luxembourg ir ETH Zurich.

Projekto eiga

Projekto įgyvendinimo planas buvo struktūrizuotas etapais ir apėmė visus pagrindinius žingsnius – nuo parengiamųjų darbų, techninės architektūros kūrimo ir komandos suformavimo iki dirbtinio intelekto komponentų kūrimo, testavimo bei vartotojo sąsajos sprendimų įgyvendinimo. Kiekvienas etapas buvo suplanuotas taip, kad veiklos būtų vykdomos nuosekliai, užtikrinant aiškų progresą, testavimą ir pasirengimą tolimesniam produkto vystymui.

1. **Gruodis** – projekto pradžia

- Projekto inicijavimas ir pagrindinių veiklų planavimas.
- Komandos formavimas ir atsakomybių paskirstymas.
- IT infrastruktūros architektūros analizė ir tinkamiausio sprendimo parinkimas (Google Cloud Platform).
- Pagrindinių projekto tikslų, uždavinių ir veiklų struktūrizavimas.

2. **Sausis–vasaris** – parengiamieji ir programavimo darbai

- IT infrastruktūros paruošimas ir diegimas pagal projekto architektūrą (CloudRun, GitHub, duomenų bazės).
- Dirbtinio intelekto programavimo pradžia ir pirmųjų modelių testavimas (LLAMA 70B, GROK2).
- NIS2 direktyvos analizė ir klausimų rinkinio sudarymas naudotojo atitikčiai įvertinti.
- Pradėtas vartotojo sąsajos dizaino kūrimas – pirmųjų dizaino “draftų“ sukūrimas (UX/UI wireframes).

3. **Kovas** – DI logikos ir vartotojo sąsajos plėtojimas

- RAG metodo integracija į sistemą.
- Dokumentų apdorojimo logikos kūrimas, segmentavimas ir analizės modelio testavimas.
- Galutinio dirbtinio intelekto modelio parinkimas remiantis testavimo rezultatais.
- Vartotojo sąsajos prototipo (wireframes) perdavimas front-end kūrimui.
- UX ir UI testavimas, dizaino patobulinimai orientuoti į galutinį produktą.

4. **Balandis** – integracija, testavimas ir tarptautinė konferencija

- Front-end prototipo programavimas ir integracija su back-end.
- DI sprendimų integravimas į visą IT infrastruktūrą.
- Sistemos testavimas realiomis sąlygomis, klaidų identifikavimas ir taisymas.
- Rekomendacijų logikos vertinimas – kokybės ir atitikimo analizė.
- Dalyvavimas tarptautinėje RSA Conference San Franciske: paskaitos, susitikimai su konkurentais (Drata, Vanta), rinkos įžvalgos, produktų palyginimai.
- Kreipimasis į University of Luxembourg ir ETH Zurich.

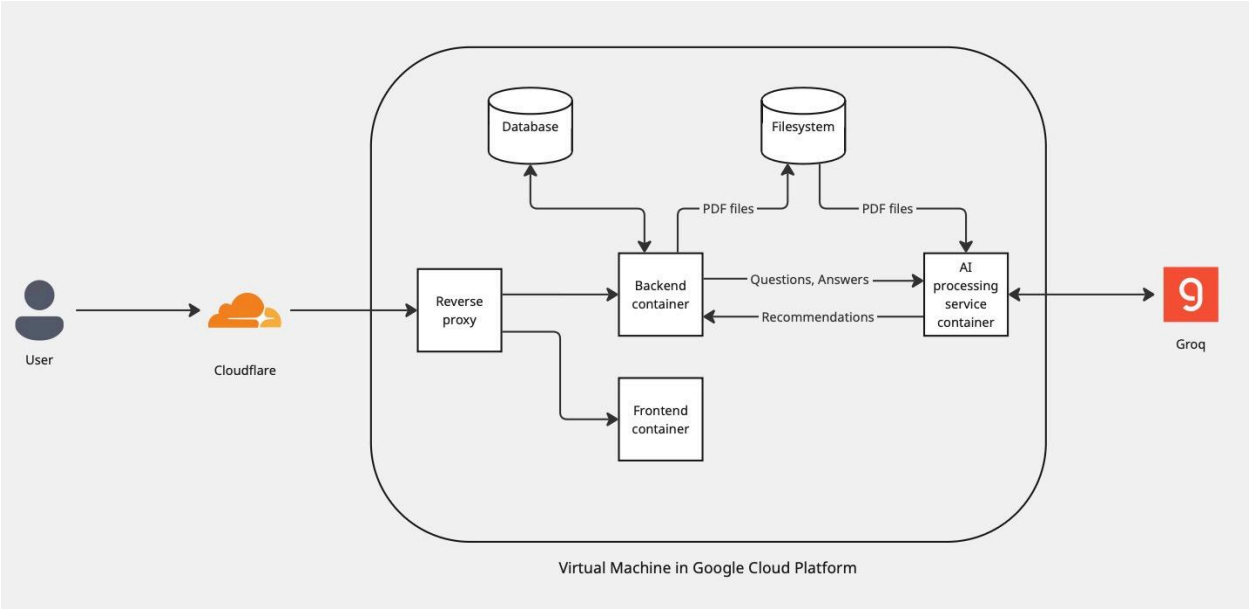
5. **Gegužė** – galutiniai darbai ir ataskaitos parengimas

- Klaidų ir spragų šalinimas, pagrindinio prototipo užtvirtinimas.

- Galutiniai testavimai su realiais duomenimis.
- UX ir UI sprendimų užbaigimas, galutinės naudotojo patirties versijos įkėlimas į Figma.
- Potencialios rinkos analizė, atsižvelgiant į surinktą informaciją iš konferencijos ir naudotojų testavimo.
- Galutinės ataskaitos parengimas.

Architektūra ir logika

Principinė aukšto lygio architektūra



Sistemos architektūra buvo kuriama kaip modulinė, debesijos pagrindu veikianti infrastruktūra, užtikrinanti lankstumą, duomenų saugumą, suderinamumą su DI komponentais ir galimybę plėstis. Visa sistema įgyvendinta „Google Cloud Platform“ (GCP) aplinkoje, pasitelkiant Cloud Run, IAM (Identity and Access Management) funkcionalumus bei kitus „serverless“ principus, o galutiniam prototipui panaudotas GCP Virtual Machine (virtualus serveris) sprendimas.

Visi duomenys apdorojami saugiai, laikantis saugumo reikalavimų (naudojamas duomenų šifravimas, prieigos kontrolė, renkami žurnaliniai įrašai) taip pat apsaugai nuo išorinių grėsmių ir atakų yra naudojamas Cloudflare sprendimas, o prieigas iš išorės užtikrininat Cloudflare Zero Trust access sprendimu.

Sistema užtikrina saugumą naudojant šiuos metodus ir sprendimus:

- Naudojamas IAM prieigų valdymui, naudojamas least-privilege principas.
- GCP aplinkoje tarp Naudotojo ir GCP visi perduodami duomenys yra šifruojami TLS 1.3.
- Saugomi duomenys (at-rest) yra šifruojami AES-256.
- Apribota prieiga iš išorės interneto.
- Apsaugai nuo išorinių atakų ir grėsmių taip pat pireigai iš išorės naudojamas Cloudflare.

Siekiant sistemos prieinamumo ilgą laiką bei suteikti stabilumo testavimams, projekto pabaigoje sukurta prototipo versija patalpinta GCP esančiame virtualiame serveryje, o ne Cloud Run. “ComplAInce” komponentai yra integruoti naudojant REST API.

Architektūra orientuota į trijų sluoksnių (angl. three-tier) logiką:

1. Vartotojo sluoksnis (front-end) - vartotojo sąsaja, leidžianti naudotojui įkelti dokumentus, atsakyti į klausimus bei peržiūrėti rezultatus.
2. Apdorojimo (serverinis) sluoksnis (backend + DI) - RAG (retrieval-augmented generation) metodika pagrįstas analizės modulis, DI modelio integracija ir semantinė paieška ir virtualaus serverio infrastruktūra.
3. Duomenų sluoksnis (vektorinė duomenų bazė + įprasta duomenų bazė ir failinė sistema) – informacijos apie NIS2 saugojimas, įkeltų dokumentų saugojimas, paieškos indeksai, klausimų ir atsakymų saugojimas.

Logikos aprašymas

1. Įvestis (input):

Naudotojas prisijungia prie sistemos ir pateikia informaciją dviem būdais:

- Įkelia įmonės dokumentus (.pdf formatas).
- Atsako į iš anksto parengtus klausimus, susijusius su NIS2 direktyvos reikalavimais (Priedas Nr. 1).

2. Embedding:

Pateikti dokumentai ir atsakymai paverčiami į vektorius naudojant *“text embedding”* algoritmus. Šiame etape sukuriamos semantinės reikšmės, kurios atspindi turinio prasmę.

3. Paieška (retrieval):

“Embedding’ai” naudojami paieškai vektorinėje duomenų bazėje (FAISS), kad būtų surasti aktualiausi fragmentai iš:

- Naudotojo įkeltų dokumentų.
- Vidinėje sistemoje įkelto NIS2 dokumento ir kitos informacijos.

4. LLM analizė:

Pasitelkiamas **LLAMA 70B** kalbos modelis, kuris suformuoja analizės atsakymą remdamasis naudotojo atsakymais į klausimus bei surastais fragmentais (RAG schema). Modelis atsako:

- Ar atsakymas / dokumentas atitinka NIS2.
- Jei ne – kokių elementų trūksta.
- Pateikia rekomendaciją, ką reikėtų pridėti ar pakeisti.

5. Rezultatas (output):

Naudotojui pateikiama aiški, struktūrizuota informacija:

- Atitikties lygis (atitinka / dalinai atitinka / neatitinka).
- Rekomenduojami veiksmai.

Prototipo kūrimas ir testavimas Ir galutinės išvados

Koncepcijos pasirinkimas

Prototipas buvo vystomas siekiant įvertinti technologinį idėjos potencialą ir galimybes – t.y. ar dirbtinio intelekto modelis gali atlikti automatizuotą dokumentų atitikties ir Naudotojo laisva forma įvestų atsakymų į klausimus analizę pagal NIS2 direktyvą. Teisės aktas pagal kurį bus lyginama atitiktis buvo pasirinktas remiantis aktualumu kritiniams sektoriams: buvo svarstyta alternatyva – DORA teisės aktas, tačiau buvo pasirinkta NIS2, nes ši direktyva yra plačiau taikoma įvairioms pramonės šakoms.

Atsižvelgiant į LLM galimybes ir turimą techninę infrastruktūrą, “ComplAInce” prototipas buvo sukurtas anglų kalba – dėl didesnio modelių efektyvumo ir tikslesnių atsakymų šia kalba.

Testuoti DI modeliai ir vertinimo kriterijai

Projekto metu buvo atlikta išsami dirbtinio intelekto modelių analizė ir praktinis testavimas siekiant nustatyti, kuris modelis geriausiai tinka NIS2 dokumentų ir atsakymų analizei. Pagrindinis tikslas – patikrinti ar realus technologinis projekto įdėjos įgyvendinimas bei rasti balansą tarp tikslumo, apdorojimo greičio, semantinio supratimo ir technologinio įgyvendinimo paprastumo.

Buvo pasirinkti ir testuojami du LLM modeliai:

- LLAMA 70B
- GROK2

Vertinimo metu buvo taikomi šie kriterijai:

- Atsakymų tikslumas (atitiktis NIS2 turiniui ir kontekstui).
- Sugeneruotų rekomendacijų vertė Naudotojui.
- Atsparumas dviprasmybėms ir netipiškoms formuluotėms.
- Generavimo greitis / tokenų apdorojimo sparta.
- Techninės integracijos sudėtingumas.

Modelių palyginimo rezultatai pateikti **Priede Nr. 2**, kur aiškiai matyti, kad LLAMA 70B pasirodė geriau:

- Tikslumas: aukštesnis semantinis supratimas, mažiau „hallucination“ tipo atsakymų.
- Kontekstinė analizė: geresnis gebėjimas susieti informaciją tarp skirtingų dokumento dalių.
- Rekomendacijų kokybė: pateikiamos aiškesnės, praktiškesnės rekomendacijos nei GROK2.

Pasirinkto DI modelio integracija ir veikimo parametrai

Galutinis sprendimas buvo naudoti LLAMA 70B modelį per GROQ tiekėją, kuris pasiūlė prieinamą kainodarą bei paprastą API integraciją:

- **Greitis:** 330 tokenų per sekundę.
- **Kaina:** 0,59 USD už 1 milijoną tokenų.
- **Apribojimai:** 30 000 tokenų per minutę (rate limiting).

Šis sprendimas pasirinktas sąmoningai – siekiant sumažinti kaštus ir išvengti infrastruktūrinių išlaidų, susijusių su nuosavos LLM sistemos kūrimu bei GPU resursų palaikymu (kas būtų ypač brangu prototipo stadijoje).

Dokumentų formatas ir apdorojimo logika

Siekiant maksimaliai padidinti sistemos stabilumą, buvo pasirinkta naudoti tik PDF dokumentų formatą, kuris užtikrina didesnį suderinamumą ir mažesnę klaidų tikimybę analizuojant failo turinį.

Naudojant dokumentus, buvo sukurta ir įgyvendinta semantinio dokumentų skaidymo ir klasifikavimo sistema, kur kiekvienas tekstinis fragmentas priskiriamas vienai iš pagrindinių NIS2 politikų kategorijų. Pagrindiniai prototipe numatyti politikų tipai:

- Risk Assessment Policy
- Incident Reporting Policy
- Incident Response Plan
- Access Control Policy
- Data Encryption Policy
- Security Monitoring Policy
- Patch Management Policy
- Business Continuity Plan
- Third-Party Risk Management Policy
- Regulatory Compliance Policy

Šis struktūrizavimas sudarė galimybę taikyti analizę, leidžiant tiek dokumentų, tiek naudotojo pateiktų atsakymų atitiktį vertinti pagal konkretų politikos kontekstą.

RAG architektūra ir FAISS vektorinė paieška

Modelio atsakymų kokybei užtikrinti buvo taikytas pažangus metodas – RAG (retrieval-augmented generation):

- Naudojant FAISS vektorinę paieškos sistemą, tekstai (tiek įkeltų dokumentų, tiek NIS2) buvo paverčiami į embedding vektorius.
- Klausimas ir dokumento analizės užklausa paverčiama į vektorių, kuris naudojamas susijusių tekstinių fragmentų paieškai duomenų bazėje.
- Fragmentai perduodami LLM kaip papildoma konteksto informacija.
- Modelis generuoja atsakymus, remdamasis aktualia, NIS2 dokumente esančia informacija.

Toks metodas ženkliai sumažino atsitiktinių ar neteisingų „hallucination“ atsakymų kiekį ir padidino rekomendacijų patikimumą.

Techniniai DI apribojimai

Nepaisant sėkmingos integracijos, buvo užfiksuoti keli praktiniai apribojimai, darantys įtaką naudojimo kokybei:

- Vieno dokumento analizės trukmė: vidutiniškai 8–12 minučių (dokumentas su 6 puslapiais generuoja apie 200–300 tūkst. tokenų).
- Vieno klausimo analizė: apie 1000–2000 tokenų, apdorojimas per ~1 minutę.
- Kelių dokumentų analizė iš eilės: sistema smarkiai sulėtėja, nes viršijamas tokenų per minutę limitas.
- Projekto metu nebuvo galimybės naudoti realaus laiko analizės režimo, o tai mažina produkto pritaikymą komercinėje aplinkoje.

DI bandymų vertinimas

Buvo įvertintas rekomendacijų tikslumas:

- **81 %** – tikslūs atsakymai iš pirmo karto.
- **13 %** – dalinai tikslūs, reikėjo papildymo.
- **6 %** – netikslūs (dažniausiai dėl “chunkinimo” ar nepakankamo įkelto dokumento filtravimo).

Nepaisant apribojimų, LLAMA 70B per GROQ platformą buvo įvertintas kaip geriausias sprendimas prototipo stadijai. Modelis užtikrino:

- Aukštą atsakymų kokybę.
- Lengvą integraciją per API.
- Pakankamą veikimo greitį MVP (minimum viable product) prototipo testavimui.

Šis technologinis testavimas leido pagrįsti, kad pasirinkta dirbtinio intelekto kryptis yra ne tik realiai įgyvendinama, bet ir turi stiprų plėtros potencialą, pritaikant ją kitoms saugumo direktyvoms ar rinkoms.

UX/UI ir naudotojo patirtis

Vienas iš projekto tikslų buvo užtikrinti, kad kuriamas prototipas būtų prieinamas ir suprantamas ne tik techniniams specialistams, bet ir organizacijų vadovams,

teisininkams, administracijos darbuotojams – t. y. tiems, kurie dažniausiai atsakingi už atitiktį, tačiau neturi gilaus technologinio ar kibernetinio saugumo išsilavinimo.

Dizaino principai ir kryptis

Prototipo naudotojo sąsaja buvo sukurta remiantis šiais principais:

- **Minimalizmas ir aiškumas** – vengiant perteklinių funkcijų ar grafinių elementų, kurie galėtų blaškyti Naudotoją.
- **Intuityvumas** – kiekvienas mygtukas, žingsnis ir pasirinkimas turi būti lengvai suprantamas iš pirmo žvilgsnio.
- **Vizualinis nuoseklumas** – naudojami vienodi elementai, spalvos, šriftai, siekiant vientisos vartotojo patirties.

UX/UI testavimas su tiksliniais Naudotojais

UX/UI sprendimai buvo vertinami atliekant Naudotojų apklausas. Tyrimas buvo vykdomas su 10 realių Naudotojų, kurie atstovavo šias grupes:

- Įmonių vadovai (be techninio išsilavinimo).
- Įmonių atitikties ar teisinio skyriaus darbuotojai.
- Administracijos darbuotojai.
- Inžinieriai ar techniniai darbuotojai (IT sektoriaus).
- Kiti, nesusiję su IT ar technologine sritimi darbuotojai.

Testavimo tikslas – išsiaiškinti realų Naudotojo elgesį, identifikuoti galimas problemas bei optimizuoti Naudotojo patirtį.

Įvertinti šie aspektai:

- **Funkcinių elementų išdėstymas**: ar Naudotojai lengvai randa mygtukus (pvz., „Įkelti dokumentą“, „Tęsti“, „Peržiūrėti ataskaitą“) ir ar jų vieta atitinka Naudotojų lūkesčius.
- **Dėmesio trajektorija**: kaip juda akys, kur pirmiausia krypsta žvilgsnis.
- **Žingsnių aiškumas**: ar aišku, ką reikia daryti kiekviename žingsnyje, ar sistema suteikia grįžtamąjį ryšį, ar nesukelia nežinios jausmo.

Gauti atsakymai ir taikymas prototipe

Testavimas buvo atliktas ir jo metu gautos įžvalgos buvo struktūrizuotai analizuojamos UI/UX dizainerio ir projekto vadovo. Išvados:

- Vartotojai tikėjosi rasti pagrindinius veiksmų mygtukus dešinėje puslapio pusėje arba žemiau aktyvaus veiksmo srities.
- Dėmesys natūraliai krypsta iš viršaus į centrą, todėl svarbiausia informacija ir nurodymai turi būti pateikti būtent toje vietoje.
- Naudotojai pageidavo, kad žingsniai būtų aiškiai suskaidyti ir turėtų pažymėtą progresą (pvz., „1 iš 4“, „Tęsti“, „Grįžti“), o ne pateikti kaip vienas ilgas formos puslapis.

Remiantis šiomis įžvalgomis:

- Sukurtas prototipas Figma platformoje su tiksliu žingsnių suskirstymu, patogia funkcinių mygtukų logika bei dizaino sprendimais.
- Pritaikytas spalvų kontrastas ir šriftų dydžiai, kad informacija būtų lengvai įskaitoma.
- Užtikrintas dizaino techninis parengimas: visi vizualiniai sprendimai perduoti programuotojui su tiksliais komponentų aprašais (wireframes, UI kit).

Dizaino failai pateikti **Priede Nr. 3**, kuriame matomi pagrindiniai Naudotojo patirties etapai: prisijungimas, dokumentų įkėlimas, klausimų pildymas, analizės peržiūra ir galutinės rekomendacijos.

UX/UI sprendimai buvo kuriami ne kaip formali funkcija, bet kaip esminė projekto dalis, užtikrinanti, kad net technologiniu požiūriu sudėtinga DI sistema būtų prieinama ir patogi bet kuriam verslo naudotojui. Surinktos tikslinės auditorijos įžvalgos leido parengti ne tik prototipą, bet ir tvirtą UX/UI pamatą galutinei, plataus masto “ComplAInce” versijai.

Techninė architektūra ir prototipo kūrimas

Projekto metu buvo įvertintos kelios debesijos infrastruktūros platformos – Amazon Web Services (AWS), Microsoft Azure ir Google Cloud Platform (GCP).

Po analizės nuspręsta naudoti Google Cloud Platform (GCP) dėl šių priežasčių:

- Techninė komandos kompetencija ir patirtis su GCP Cloud Run paslauga, leidžiančia greitai diegti konteinerizuotas aplikacijas.
- Cloud Run užtikrino automatinį resursų paskirstymą ir horizontalų mastelį, leidžiantį sistemai prisitaikyti prie skirtingo apkrovimo – ypač naudinga testuojant DI modelių apkrovą.
- Egzistuojantis “MB AG Cyber” GCP mokėjimo planas, leidžiantis naudotis debesijos resursais ekonomiškai ir efektyviai.

- Paprastas API integravimas su išoriniais dirbtinio intelekto tiekėjais, ypač testuojant GROQ integraciją.
- Saugumo funkcionalumas – GCP siūlo integruotą IAM (Identity and Access Management) sistemą, kuri leidžia centralizuotai valdyti prieigos teises pagal naudotojų vaidmenis ir atsakomybę.

Naudotos technologijos

Projekto integravimo ir programavimo darbams buvo pasitelktos šios technologijos:

- **Backend dalis**: sukurta naudojant Spring Boot ir Kotlin – tai patikimas ir lankstus technologinis sprendimas, leidžiantis efektyviai dirbti su duomenimis, DI moduliais per dedikuotus servisus ir API sąsajomis.
- **Frontend dalis**: realizuota su Angular framework, leidžiančiu greitai kurti interaktyvias Naudotojo sąsajas, atitinkančias UX/UI reikalavimus ir Wireframes informaciją.

Naudotojo patirtis sistemoje (User Flow)

Sukurtas prototipas užtikrina patogią ir logiškai suskirstytą Naudotojo patirtį:

1. Prisijungimas prie sistemos.
2. Dokumentų įkėlimas PDF formatu.
3. Klausimyno pildymas.
4. Automatinė analizė su rekomendacijomis ir ataskaita.

Duomenų saugumas ir privatumas

Visi Naudotojų duomenys ir dokumentai yra apdorojami saugiai, laikantis aukščiausių informacijos saugumo reikalavimų. Sistema užtikrina saugumą naudodama šias priemones:

- Duomenų šifravimas tiek saugojimo metu (at rest), tiek perdavimo metu (in transit).
- IAM (Identity and Access Management) – ribojama prieiga pagal naudotojų vaidmenis.
- Žurnalinių įrašų (audit logs) kaupimas – kiekvienas prisijungimas, dokumento įkėlimas ar analizės paleidimas yra registruojamas.
- Apsauga nuo išorinių grėsmių: naudojama Cloudflare infrastruktūra, kuri apsaugo nuo DDoS atakų, bot srauto, nesankcionuotų skenavimų.

- Cloudflare Zero Trust Access – prieiga prie vidinės sistemos leidžiama tik autentifikuotiems naudotojams per saugius tinklo tunelius, užtikrinant, kad net atakuojant iš išorės nebūtų galimybės pasiekti aplikacijų tiesiogiai.
- API raktai ir token'ai – naudojami visoms vidinėms ir išorinėms DI bei vektorinių paieškų integracijoms.

Šis architektūrinis sprendimas leidžia pasiekti balansą tarp veikimo efektyvumo, plėtros lankstumo ir kibernetinio saugumo reikalavimų laikymosi, kas yra esminis aspektas NIS2 atitikties įrankio kontekste

Užbaigtas projekto prototipas pateikiamas **Priede Nr. 4**

Galutiniai naudotojų atsiliepimai ir įžvalgos

Projekto metu, pasibaigus techninių testų etapui, buvo atliktas prototipo demonstravimas ir testavimas su tiksliniais galutiniais Naudotojais – įmonių vadovais, IT specialistais, bei žmonėmis, neturinčiais gilios patirties IT. Atsiliepimai buvo renkami pokalbių ir interaktyvaus testavimo būdu, vertinant realią naudotojo patirtį ir prototipo funkcionalumą.

Apibendrintos pagrindinės vartotojų įžvalgos:

- **Veikimo greitis**

Naudotojai teigiamai įvertino įrankio koncepciją, tačiau dažniausiai pasikartojęs pastebėjimas buvo susijęs su veikimo greičiu:

„Geras įrankis, bet per lėtas.“

Šis pastebėjimas atspindi dabartinius technologinius apribojimus, susijusius su DI apdorojimo greičiu naudojant išorinį tiekėją (GROQ) su tokenų perdavimo limitais. Tai patvirtina būtinybę tolimesnėje plėtroje investuoti į nuosavą LLM infrastruktūrą.

- **Duomenų saugumas ir privatumas**

Dalis naudotojų išreiškė susirūpinimą dėl dokumentų siuntimo į trečiųjų šalių DI modelius:

„Reikia daugiau saugumo – kad nebūtų siunčiama į trečiųjų šalių DI modelius.“

Šis poreikis aiškiai nurodo svarbą ateityje pasiūlyti pilnai lokalizuotą (on-premise) arba uždaro debesijos sprendimo versiją, ypač klientams iš reguliuojamų sektorių (finansai, medicina, kritinė infrastruktūra).

- **Lokalizacija (lietuvių kalba)**

Prototipo versija veikė tik anglų kalba (dėl LLAMA modelio apribojimų ir testavimo tikslingumo). Vartotojai pabrėžė poreikį lokalizuoti sistemą:

„Turėtų būti prieinamas ir lietuvių kalba.“

Ateityje būtina integruoti lokalizuotą sąsają ir dirbtinio intelekto atsakymus generuoti vietine kalba.

- **Tikslumas ir pasitikėjimas rezultatais**

Vartotojai tikisi aukšto tikslumo – ypač tais atvejais, kai sprendimai remiasi pateikiamomis rekomendacijomis, turinčiomis įtakos atitikties įrodymams ar verslo rizikai:

„Norėtųsi beveik 100 % tikslumo“

Ši įžvalga parodo, jog galutinis produktas turi būti paremtas ne tik pažangiu DI sprendimu, bet ir papildomu verifikacijos sluoksniu – pvz., žmogaus peržiūra arba dvigubu validavimo mechanizmu (angl. human-in-the-loop).

Konferencija, bendradarbiavimas ir rinkos analizė

Partnerystės su universitetais

Vadovaujantis projekto paraiškoje numatytais įsipareigojimais ir siekiant užmegzti potencialų bendradarbiavimą tarptautiniam konsorciumui ateityje (pvz., teikiant paraiškas pagal “Europos horizontas“ programą), buvo inicijuoti oficialūs kontaktai su dviem Europos mokslinių tyrimų institucijomis – University of Luxembourg ir ETH Zurich.

Visgi, nepaisant išsiųstų kreipimųsi, iš nė vienos institucijos nebuvo gauta atsakymų ar susidomėjimo prisijungti prie projekto šiuo etapu. Atsižvelgiant į tai, buvo priimtas sprendimas tęsti projektą be akademinių partnerių, koncentruojantis į technologinio prototipo sukūrimą ir realių naudotojų poreikių įvertinimą.

Dalyvavimas tarptautinėje RSA konferencijoje

Projekto vadovas dalyvavo RSA Conference 2024 (San Franciske), kuri yra viena didžiausių ir svarbiausių kibernetinio saugumo tematikos konferencijų pasaulyje. Konferencijoje buvo:

- Dalyvauta paskaitose apie DI ir kibernetinį saugumą, tarp jų ir aktuali sesija:

DevOps Connect Seminar — "AI and Security: Transforming Modern AppDev",

Sesijoje buvo nagrinėjama DI įtaka saugumo sprendimų kūrimui ir integracijai į programinės įrangos kūrimo ciklą.

- Atlikta konkurencinės aplinkos analizė, įvertinant esamų sprendimų rinką. Buvo nagrinėti didžiųjų žaidėjų – tokių kaip "Drata" ir "Vanta" – sprendimai. Šios įmonės siūlo pažangius „GRC" (Governance, Risk, Compliance) ir kibernetinio atitikties produktus didelėms organizacijoms.

Pagrindinės įžvalgos:

- Šie sprendimai remiasi panašia logika: klausimynų pildymas, dokumentų įkėlimas ir analizė, bei rizikos vertinimas.
- Nei "Drata", nei "Vanta" neturi koreliacijos mechanizmo tarp dokumentų analizės rezultatų ir pateiktų atsakymų – tai yra funkcionalumas, kuris yra planuojamas įgyvendinti galutiniame "ComplAInce" produkte, jei pavyks patekti į "Europos horizontas" programą. Ši funkcija gali tapti esminiu "ComplAInce" konkurenciniu pranašumu.

Taip pat nustatyta, kad:

- Esami konkurentų sprendimai orientuoti į enterprise lygio klientus, yra brangūs bei reikalauja išsamaus diegimo.
- Jų vartotojo sąsajos yra kompleksiškos, skirtos pažengusiems naudotojams ar IT padaliniams, apkrautos daug papildomų funkcijų.

"ComplAInce" projekto unikalumas – tai paprastumas, greitis, minimalizmas, suprantama kalba ir prieinamumas vidutinio dydžio ir nedidelėms organizacijoms, neturinčioms didelių žmogiškųjų ir finansinių resursų.

Finansuoja Europos Sąjunga
NextGenerationEU

Rinkos analizės išvados

Atlikta rinkos analizė parodė, kad šiuo metu rinkoje nėra sprendimo, kuris būtų tiesiogiai analogiškas “ComplAInce” prototipui – ypač kalbant apie kombinaciją:

- Automatinė dokumentų analizė naudojant DI.
- Integruotas klausimynas ir atitikties rekomendacijos.
- Paprastas, vizualiai aiškus naudotojo kelias.
- Neturėjimas papildomų funkcijų, kurios sprendžia kitas, nesusijusias problemas.

Šiuo metu esami sprendimai dažniausiai yra:

- Skirti didelėms, reguliuojamoms įmonėms.
- Sukurti kaip didelės platformos.
- Riboto prieinamumo mažoms ar valstybinėms organizacijoms dėl kaštų ir įgyvendinimo bei naudojimo sudėtingumo.

Išvada: “ComplAInce” sprendimas turi didelį potencialą tapti nišiniu produktu, skirtu reguliuojamų sektorių (fintech, sveikatos, kritinės infrastruktūros) mažoms ir vidutinėms įmonėms, kurios ieško:

- Greito,
- Aiškaus,
- Lokaliai pritaikyto (pvz., kalba),
- Ir funkcionaliai tikslaus DI pagrindu veikiančio atitikties įrankio.

Tai sukuria stiprų pagrindą tolesnei produkto plėtrai bei sėkmingai paraiškai “Europos horizontas” kvietimuose.

Išvados ir rezultatai

Remiantis atliktais darbais, galima teigti, kad visi esminiai uždaviniai buvo įgyvendinti, o tikslai – pasiekti. Projektas „ComplAInce“ sėkmingai įrodė technologinio sprendimo – remiamo dirbtiniu intelektu, RAG architektūra ir robotine procesų automatizacija – veikimą bei realų pritaikymą analizuojant dokumentų atitiktį pagal NIS2 direktyvą.

Techninės išvados:

Sukurtas prototipas efektyviai analizuoja naudotojo įkeltus dokumentus ir atsakymus į klausimus, pasitelkdama RAG modelį ir pažangų LLM – LLAMA 70B, kuris buvo pasirinktas po palyginamojo testavimo su GROK2 modeliu. Implementuota vektorinė

paieška (FAISS) užtikrino semantinį atitikimą net ir esant dviprasmybėms, o dokumentų skaidymas ir klasifikavimas leido padidinti analizės tikslumą. Nepaisant techninių apribojimų (pvz., apdorojimo greitis ir tokenų limitai), pasiektas pakankamas sistemos efektyvumo lygis MVP prototipui.

Naudotojo patirties išvados:

Prototipas buvo sukurtas su aiškiu UX/UI – testuotas su tiksliniais Naudotojais, įskaitant specialistus be technologinės patirties, kuriems sistema buvo suprantama ir paprasta naudoti. Surinkti atsiliepimai padėjo optimizuoti Naudotojo sąsają, užtikrinant intuityvų funkcionalumą. Gauta kritika dėl greičio, kalbos lokalizacijos ir duomenų saugumo parodė kryptis tolimesniam tobulinimui.

Rinkos potencialas:

Atlikta konkurencinė analizė parodė, kad tokio tipo sprendimai egzistuoja enterprise segmente ir dažnai yra per sudėtingi ar per brangūs mažoms ir vidutinėms įmonėms. „ComplAInce“ išsiskiria savo paprastumu, gera naudotojo patirtimi, rekomendacijų aiškumu ir galimu lokalizavimu, todėl turi didelį potencialą – ypač reguliuojamuose sektoriuose (pvz., medicinos, energetikos, finansų) bei mažų ir vidutinių įmonių segmente.

Atitikimas tikslams:

- ***Technologinės galimybės ištirtos:*** įgyvendintas pilnai veikiantis prototipas su DI analize, integracijomis ir dokumentų apdorojimu.
- ***Prototipas sukurtas ir ištestuotas:*** sistema realiai atlieka analizę, generuoja ataskaitas ir rekomendacijas pagal NIS2.
- ***LLM modelių ir architektūros vertinimas atliktas:*** testuoti 2 modeliai, įgyvendinta RAG struktūra.
- ***UX/UI prototipas sukurtas ir įvertintas:*** dizainas pritaikytas realiems Naudotojams, testuotas ir perdavus programuotojams - įgyvendintas.
- ***Rinkos ir technologinė analizė atlikta:*** įvertinti konkurentai, išskirtos galimos nišos ir pranašumai.
- ***Parengtas pagrindas “Europos horizontas“ programai:*** sukurtas pagrįstas pagrindas paraiškai teikti.

Apibendrinimas:

„ComplAInce“ projektas įgyvendintas sėkmingai. Sukurtas ir ištestuotas prototipas, kuris įrodė dirbtinio intelekto pagrindu veikiančio dokumentų ir atsakymų atitikties analizės

sprendimo technologinį gyvybingumą ir praktinę vertę. Projekto rezultatai sudaro stiprų pagrindą produkto komercializavimui bei tolesniam plėtojimui per Europos inovacijų finansavimo programas.

Deklaracija

Visos projekto veiklos buvo įgyvendintos pagal paraišką ir sutartį. Pasiektas pagrindinis tikslas – patikrinta DI pagrįsto NIS2 atitikties tikrinimo sprendimo idėja, kuri pasirodė perspektyvi tiek technologiniu, tiek rinkos požiūriu.

Priedas Nr. 1 – NIS2 klausimai

General Cybersecurity Governance

- Does the organization have a documented cybersecurity policy in place?
- Is there a designated individual (e.g., CISO) responsible for overseeing cybersecurity compliance?
- Are cybersecurity roles and responsibilities clearly defined across the organization?
- Has a risk assessment been conducted within the last 12 months?
- Are there procedures for regularly reviewing and updating cybersecurity policies?

Access Control

- Are user access privileges assigned based on the principle of least privilege?
- Is multi-factor authentication (MFA) implemented for all critical systems and remote access?
- Are inactive user accounts disabled or removed within a specified timeframe (e.g., 90 days)?
- Is there a process for reviewing and revoking access when an employee leaves the organization?
- Are privileged accounts (e.g., admin accounts) monitored and audited regularly?

Data Protection

- Is sensitive data (e.g., PII, PHI, financial data) identified and classified?
- Are encryption mechanisms in place for data at rest and in transit?
- Is there a data retention policy that specifies how long data is stored and when it is destroyed?
- Are backups of critical data performed regularly and stored securely?
- Is there a process for detecting and responding to data breaches?

Network Security

- Are firewalls and intrusion detection/prevention systems (IDS/IPS) deployed and actively monitored?
- Is network traffic segmented to limit the spread of potential breaches?
- Are wireless networks secured with strong encryption (e.g., WPA3)?
- Is there a process for monitoring and logging network activity?
- Are penetration tests or vulnerability scans conducted at least annually?

Incident Response

- Does the organization have a documented incident response plan?
- Are employees trained on how to report security incidents?
- Is there a defined process for investigating and mitigating cybersecurity incidents?
- Are incident response activities tested through tabletop exercises or simulations?
- Are post-incident reviews conducted to identify lessons learned and improve processes?

Employee Training and Awareness

- Are all employees required to complete cybersecurity awareness training annually?
- Is there a process to educate staff about phishing and social engineering threats?
- Are policies regarding acceptable use of company devices and systems communicated to employees?
- Are contractors and third-party vendors held to the same cybersecurity standards as employees?
- Is there a mechanism to track training completion and compliance?

Third-Party Risk Management

- Are third-party vendors assessed for cybersecurity risks before onboarding?
- Do contracts with vendors include cybersecurity requirements and compliance obligations?
- Is there ongoing monitoring of third-party compliance with security standards?
- Are third-party access rights to systems and data regularly reviewed?
- Has a supply chain risk management plan been established?

Compliance and Auditing

- Are regular internal audits conducted to verify compliance with cybersecurity policies?
- Has an external audit or certification (e.g., SOC 2, ISO 27001) been completed in the past year?
- Are findings from audits tracked and remediated within a specified timeframe?

- Is there documentation proving compliance with applicable regulations (e.g., GDPR, CCPA)?
- Are logs and records maintained for the required retention period (e.g., 3-7 years)?

Physical Security

- Are physical access controls (e.g., badges, locks) in place for facilities housing critical systems?
- Is there a process for monitoring and logging physical access to sensitive areas?
- Are portable devices (e.g., laptops, USB drives) encrypted and tracked?
- Are hard copies of sensitive data stored securely and disposed of properly?
- Are security cameras or other monitoring systems in place where required?

Software and System Security

- Are all systems and software updated with the latest security patches?
- Is there an inventory of all hardware and software assets in use?
- Are secure development practices (e.g., code reviews, testing) followed for in-house applications?
- Is antivirus/malware protection installed and up to date on all endpoints?
- Are end-of-life systems replaced or isolated to mitigate risks?

Priedas Nr. 2 – LLM modelių palyginimas

Modelių Palyginimo Lentelė (LLAMA vs GROK2)		
Parametras	**LLAMA 70B**	**GROK2**
Kūrėjas	Meta	xAI (Elon Musk)
Tikslumas (NIS2 atitikčiai)	~81 %	~62 %
Konteksto valdymas	Aukštas – gerai seka temų, sakinių, žodžių ryšius dokumente	Vidutinis – dažnai nesusieja skirtingų informacijos fragmentų
Reikalavimų klasifikacija	Veiksminga – gerai atpažįsta politikų tipus	Ribota – dažnai neatlieka kontekstinio priskyrimo tinkamai politikai
Rekomendacijų kokybė	Detalios, konkrečios, pagrįstos dokumento turiniu	Bendrinės, nekonkrečios, dažnai netinkamos praktiniam sprendimui
Integracijos sudėtingumas	Reikalingi dideli techniniai resursai, sudėtingesnė API	Paprastesnė integracija, tinka greitam prototipavimui
Tinkamumas RAG architektūrai	Labai gerai suderinamas – optimizuotas su embedding'u	Prastai derinamas – sunku pritaikyti retrieval elementams

Modelių Palyginimo Lentelė (LLAMA vs GROK2)		
Parametras	**LLAMA 70B**	**GROK2**
Kūrėjas	Meta	xAI (Elon Musk)
Tikslumas (NIS2 atitikčiai)	~81 %	~62 %
Konteksto valdymas	Aukštas – gerai seka temų, sakinių, žodžių ryšius dokumente	Vidutinis – dažnai nesusieja skirtingų informacijos fragmentų
Reikalavimų klasifikacija	Veiksminga – gerai atpažįsta politikų tipus	Ribota – dažnai neatlieka kontekstinio priskyrimo tinkamai politikai
Rekomendacijų kokybė	Detalios, konkrečios, pagrįstos dokumento turiniu	Bendrinės, nekonkrečios, dažnai netinkamos praktiniam sprendimui
Integracijos sudėtingumas	Reikalingi dideli techniniai resursai, sudėtingesnė API	Paprastesnė integracija, tinka greitam prototipavimui
Tinkamumas RAG architektūrai	Labai gerai suderinamas – optimizuotas su embedding'u	Prastai derinamas – sunku pritaikyti retrieval elementams

Priedas Nr. 3 – UX/UI dizainas

Nuoroda į FIGMA:

https://www.figma.com/design/VkVP6o1z2Xjh0R6YPYVdgB/ComplAInce-Product?node-id=606-54332

Priedas Nr. 4 – "ComplAInce" prototipas

Nuoroda į prototipą:

https://dev.acprojects.eu/

SVARBU: Prototipas yra apsaugotas. Norint gauti prieigą prie prototipo aplinkos, reikalinga susisiekti su projekto vadovu kontaktais:

NAUJOS KARTOS
LIETUVA

ACyber

Email: antanas@acyber.io
Tel: +370 654 27982

Finansuoja
Europos Sąjunga
NextGenerationEU