

Johdanto

Tämä tietoturvakuvaukset kattaa ProjectTOPin toiminnot, jotka käyttävät OpenAI:n API:a AI-toimintojen toteuttamiseen. Kuvauksessa käsitellään toiminnallisuus, tietojen valinta, tietojen suojaus, tietoturvariskit ja parhaita käytäntöjä tietoturvan varmistamiseksi.

Yleiskuvaus

ProjectTOPin AI-toiminnot toimivat samalla periaattella:

1. Käyttäjältä pyydetään tietoja (tekstisyöte tai muita tietoja kuten lisäkenttien valinta)
2. Käyttäjän antamien tietojen perusteella muodostetaan kehote seuraavasti:
 - a. Kehote OpenAI:lle muodostuu järjestelmän, konfiguraation ja käyttäjän kehoitteista sekä valituista tiedoista. (esim. aktiviteetin kuvaus, lisäkentät)
 - b. Tähän poikkeuksena on projektin analysointi -toiminto, joka koostaa myös projektista sekä pseudonymisoitua tietoa, että tarkkaa tietoa haluttaessa
3. Muodostettu kehote lähetetään OpenAI:n API:lle ja vastauksesta muodostetaan joko strukturoitua data tai tekstimuotoista data, jotka voidaan tallentaa käyttäjän toimesta järjestelmään

ProjectTOPin 3.44 versiosta alkaen AI-toiminnot vaativat käyttöoikeusroolin (AI Basic ja AI Advanced) asetuksen käyttäjälle.

Konfiguraatioon (admin) voidaan määritellä toiminnoille lisäkehote, joka lähetetään jokaisen kehoitteen mukana.

Pääsyhallinta ja autentikointi

- OpenAI API:iin yhteys muodostetaan ProjectTOPin hallinnoimalla API-avaimella
- API-avaimet ovat asiakaskohtaisia ja niiden pääsy on rajattu vain tarpeellisiin palveluihin
- ProjectTOPin versioissa ≥ 3.44 voidaan määritellä asiakkaan oma OpenAI API-avain, jota käytetään ProjectTOPin avaimen sijasta

Tietojen suojaus ja salaus

- Kaikki tietoliikenne OpenAI:n API:n ja ProjectTOPin välillä on suojattu TLS 1.3 -salauksella. ProjectTOPin ohjelmiston selaimen ja palvelimen välinen tietoliikenne on niin ikään suojattu TLS1.3 -salauksella.
- Kaikki tietoliikenne OpenAI:n API:n ja ProjectTOPin välillä tapahtuu palvelinyhteytenä eli käyttäjillä ei ole pääsyä API-avaimeen
- Oletuksena käyttäjän antamista tiedoista tarkkaillaan henkilötunnuksen (Suomi) muotoista tekstiä ja luottokortin numeroita. Mikäli näitä löydetään, estetään kehoitteen lähetys. Tätä voidaan muuttaa konfiguraatiossa admin-tason käyttäjien toimesta (ns. regex matching).
- AI-toiminnoissa käytettyjä kehoitteita tai tuloksia ei tallenneta erikseen (pl. lokitus) mihinkään

Tietojen sijainti

- Lähtökohtaisesti ProjectTOPiin tallennetut tiedot sijaitsevat Suomessa, suomalaisessa konesalissa – AI-toiminnot poikkeavat tästä
- Alkaen ProjectTOPin versiosta 3.45.8 AI-toiminnot käyttävät hyödyksi Azure OpenAI -palvelua. Data sijaitsee EU-alueella

Lokitus ja valvonta

- ProjectTOPin AI:n ja OpenAI:n API:n käyttöä lokitetaan järjestelmään tavanomaisten ProjectTOPin lokituskäytäntöjen tapaan
- Valvontaa suoritetaan ProjectTOPin omien API-avaimien väärinkäytön estämiseksi

Riskienhallinta ja uhkien torjunta

- Suurin osa ProjectTOPin AI-toiminnoista (pl. allaoleva) lähettää vain sellaista tietoa ulos ProjectTOPista (OpenAI:lle), jota käyttäjä on sille antanut
- AI-toimintojen käyttäjät voi valita käyttöoikeuksilla ja näin voidaan estää esimerkiksi AI-käyttöön kouluttamattomien käyttäjien pääsy toimintoihin
- Vain “projektin analysointi” -toiminto kerää ja lähettää sellaista tietoa OpenAI:n API-rajapintaan, joita käyttäjä ei ole voinut erikseen valita kehotteeseen. Tämän takia ko. toiminto (ja mahdolliset vastaavat tulevaisuudessa toteutettavat toiminnot) on erillisen käyttöoikeuden takana
- AI-mallit voivat tuottaa mahdollisesti väärää tietoa eikä niiden tuottamaa informaatiota pidä käyttää sellaisenaan ilman ihmisen tarkistusta.
- Käyttäjien koulutus on tärkeä osa turvallista AI:n käyttöä. Käyttäjien tulisi huomata GDPR:n mukainen tietojenkäsittely sekä esim. liikesalaisuuksien jättäminen pois kehotteista

Päätös

ProjectTOPin AI-toiminnot on pyritty tekemään mahdollisimman turvallisiksi ja joustaviksi tämän tietoturvakuvauksen mukaisilla toimenpiteillä. ProjectTOPin AI-toiminnot käyttävät asianmukaisia suojauksia, asiakaskohtaisia API-avaimia ja käyttöoikeusrooleja tietoturvan varmistamiseksi. Järjestelmän tiedot pysyvät edelleen Suomessa, mutta AI-toiminnot voivat käyttää OpenAI:n globaaleja palvelimia, eikä AI:n tuottamaa dataa tule käyttää tarkistamatta.