Kyberturvallisuuden itsearviointityökalun tietosuoja ja turvallisuus

samk

roboAI

KYBERTURVALLISUUDEN ITSEARVIOINTITYÖKALUN TIETOSUOJA JA TURVALLISUUS

Kyberturvallisuuden itsearviointityökalun tietosuoja

Satakunnan ammattikorkeakoulun RoboAI:n Kyberturvallisuuden itsearviointityökalun verkkosivusto ja työkalu sijaitsevat Vercel-palvelutarjoajan palvelussa. Vercel hyödyntää palvelussaan Amazonin AWS infrastruktuuria. Itsearviointityökalu toimii fyysisesti AWS:n Tukholman konesalista (AWS EU-North-1).

Kyberturvallisuuden itsearviointityökalun käyttäjien tietojen ja arviointitulosten yksityisyyden suojaaminen on RoboAI:n ensisijainen tavoite. Tästä syystä itsearviointityökalun verkkopohjaiset sovellustyökalut käsittelevät ja tallentavat kaikki käyttäjätiedot ja raportit ainoastaan loppukäyttäjän selaimeen.

Tämä tarkoittaa, että Kyberturvallisuuden itsearviointityökalun-tietoja ja arviointiraportteja ei koskaan vastaanoteta, käsitellä tai tallenneta palvelimelle, joka isännöi itsearviointityökalua.

Kyberturvallisuuden itsearviointityökalu-verkkosovellus toimii ainoastaan asiakaspään (client-only) sovelluksena. Käyttääkseen työkalua käyttäjällä pitää olla laitteessaan selain ja toimiva internetyhteys.

Kun käyttäjä avaa verkkoselaimensa ja syöttää Kybeturvallisuuden itsearviointityökalu-verkkosivuston osoitteen, pyyntö käynnistyy, jolloin verkkopalvelin lähettää HTML-tiedoston ja siihen liittyvät kuvat, tyyli- ja javascript-tiedostot käyttäjän selaimeen. Kun käyttäjän selain on hakenut HTML-tiedoston, verkkosivustoa voidaan käyttää.

KYBERTURVALLISUUDEN ITSEARVIOINTITYÖKALUN TIETOSUOJA JA TURVALLISUUS

Kuten kaikilla verkkosivustoilla, myös Kyberturvallisuuden itsearviointityökalu-verkkosovelluksella on omat tiedostot eri toimintojen suorittamiseen, mukaan lukien seuraavat:

- Cascading Style Sheet (CSS) -tiedosto määrittää verkkosivun sisällön ulkoasun ja muotoilun.
- JavaScript-tiedostot määrittävät verkkosovelluksen yksinkertaiset toiminnot (esim. painikkeen painaminen laukaisee toiminnon).
- Muut tiedostot tukevat kuvien, Excel-tiedostot jne. näyttämistä käyttäjän selaimessa (tekniset tiedot on esitetty liitteessä A).

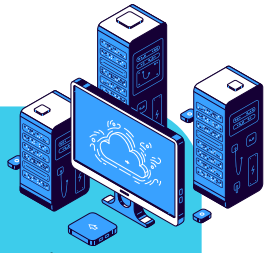
Kaikki yllä mainitut tiedostot on tallennettu Vercelin palveluun. Kun käyttäjä avaa Kyberturvallisuuden itsearviointityökalu-verkkosovelluksen, nämä tiedostot haetaan palvelimelta, jotta verkkosovellus voidaan näyttää käyttäjän selaimessa. Kun käyttäjä käyttää Kyberturvallisuuden itsearviointityökalua, kaikki käyttäjän syöttämät tiedot pysyvät käyttäjän selaimen välimuistissa (eli varatussa tallennustilassa) eikä niitä lähetetä Vercelin palveluun.

Se, miten komennot jaetaan käyttäjän tietokoneen ja Vercelin palvelimen välillä, on esitetty yksinkertaisessa kaaviossa (kuva 1). On tärkeää huomata, kuten kuva 1 osoittaa, että tietoja ei siirretä käyttäjän selaimesta / tietokoneesta Vercelin palvelimelle. Itsearviointityökalu-verkkosovelluksen palvelimella ei ole kykyä vastaanottaa ja tallentaa käyttäjätietoja (katso liite A teknisiä lisätietoja varten).

Tästä syystä on käyttäjän vastuulla tallentaa ja säilyttää arviointitietonsa ja -raporttinsa omalla tietokoneellaan käyttämällä Itsearviointityökalun Tallenna-toimintoa.

SELAIN

Kaikki asiakastiedot tallennetaan asiakkaan paikalliseen tallennustilaan ja käsitellään asiakkaan laitteella.



VERCEL

Vercel-palvelin voi ainoastaan vastaanottaa ja vastata tiedostopyyntöihin. Se ei voi vastaanottaa eikä tallentaa asiakastietoja.

Syötä itsearviointityökalun verkkosivuston osoite.

Kun asiakaspyyntö on suoritettu, verkkosivuston etusivu haetaan palvelimelta (/index.html).

Verkkosovellus pyytää tiedostot, jotka tarvitaan verkkosivuston näyttämiseen tietokoneella. Toisin sanoen pyyntö koskee HTML-tiedostossa lueteltuja skripti- ja tyylitiedostoja.

Palvelin lähettää sitten ohjelmistotiedostot (kirjoitettu JavaScript-kielellä) ja tyylitiedostot (kirjoitettu CSS-kielellä) takaisin asiakkaalle.

Käyttäjän toiminnot (esimerkiksi staattisten PDF- ja kuvatiedostojen katselu) johtavat ohjelmoituun pyyntöön tyyleille, skripteille/ohjelmille ja medialle

Kun palvelin saa pyynnön mediatiedostosta tai skriptistä/ohjelmasta, se lähettää tiedoston asiakkaalle. Huomaa, että tässä vuorovaikutuksessa ei lähetetä käyttäjätietoja. Tämä vuorovaikutus tarkoittaa vain sitä, että asiakas pyytää tiedostoja palvelimelta, jotta asiakaspuoli voi toimia ilman tarvetta palvelimelle. Palvelin ei koskaan vastaanota käyttäjätietoja.

Ohjelmallinen data pyydetään käyttäjän vuorovaikutuksen perusteella. Kaikki päätökset dynaamisten tiedostojen pyytämisestä tehdään asiakaspuolen skripteillä. Missään vaiheessa palvelimelle ei anneta käyttäjätietoja. Lisäksi palvelimella ei ole mitään keinoa tietää, missä tilassa asiakas on, miten asiakasjärjestelmä toimii tai mitä tietoja asiakkaalla on tallennettuna.

Kuva 1. Kuva tiedonvaihdosta selaimen (eli käyttäjän) tietokoneen ja Vercelin välillä.

KYBERTURVALLISUUDEN ITSEARVIOINTITYÖKALUN TIETOSUOJA JA TURVALLISUUS

Palvelimen turvallisuusvaatimustenmukaisuus ja turvallinen suunnittelu (Secure-by-Design) Kyberturvallisuuden itsearviointityökalu-verkkosivustolle

RoboAI käyttää automaattisia skannereita työkalun käyttämien kirjastojen turvallisuuden varmistamiseksi.

Liite A: Kysymykset ja vastaukset

K1. Miten Excel-raportti luodaan?
Excel-tiedosto generoidaan selaimessa toimivalla Javascript-kirjastolla, joka on erikoistunut Excel-tiedostojen generointiin (Excel.js).

K2. Mitä evästeitä käytetään?
Palvelussa ei käytetä evästeitä (cookies). Palvelujen välttämättömien toimintojen toteuttamiseen käytetään erikseen selaimen SessionStoragea.

Web-analytiikka
Tilastoimme palvelun käytöstä ainoastaan hyvin yleisluonteista dataa.
Tilastoidut asiat:
Käyttäjän sijainti (maa)
Käyttäjän päätelaite (tietokone, puhelin)
Käyttäjän selain (Chrome, Safari, Firefox)
Käyttäjän käyttöjärjestelmä (Mac, Windows, Android, iOS)
Minkä sivuston linkin kautta on palveluun saavuttu (Referers)
Millä sivuilla palvelussa on käyty

Lisätietoja käytössä olevasta Web-analytiikkapalvelusta:
https://vercel.com/docs/analytics/privacy-policy

KYBERTURVALLISUUDEN ITSEARVIOINTITYÖKALUN TIETOSUOJA JA TURVALLISUUS

K3. Mitä selaimen asiakaspuolen tallennustiloja käytetään?

Chatbotin (lisäominaisuus) osalta käytössä on SessionStorage, joka on selainpohjainen tallennustila ja se säilyttää tietoja vain istunnon ajan. Chat-istunnon tila säilytetään käyttäjän selaimessa ja palvelin ei tallenna tilatietoja. Chatbotin tallennustilaa kutsutaan nimellä aiStorage. Selaimen sulkeminen poistaa kaikki tiedot.

Muilta osin käytössä on LocalStorage, jossa tiedot pysyvät tallessa, kunnes käyttäjä poistaa ne joko itsearviointityökalun painikkeesta tai tyhjentämällä sivuhistorian.

LocalStorage sisältää kolme erilaista storagea:

- appStore: Pidetään kirjaa sovelluksen tilan tiedoista.
- assessmentStore: Pidetään kirjaa itsearvioinnin tiedoista.
- organizationStore: Pidetään kirjaa organisaation tiedoista.

Näiden tallennusmekanismien avulla varmistetaan, että käyttäjän tiedot säilyvät tarpeen mukaan joko väliaikaisesti istunnon ajan tai pysyvästi, kunnes ne poistetaan manuaalisesti. Tämä mahdollistaa joustavan ja tehokkaan tietojen hallinnan sovelluksessa.