TRIVORE

Outnumbered: viisi kysymystä agenteista

Yhden sivun itsearviointi: miten hallitsette tekoälyagenttejanne

Mika Aromaa, toimitusjohtaja, Trivore · Cyber Security Nordic 2026, Helsinki 28.–29.10.2026

Alan arvioiden mukaan yrityksissä on keskimäärin noin 45 koneidentiteettiä – palvelutunnuksia, API-avaimia, botteja ja nyt tekoälyagentteja – jokaista työntekijää kohden, ja lähes puolet niiden tunnuksista on vaihtamatta yli vuoden. Jokaisella ihmisellä on esihenkilö ja viimeinen työpäivä; useimmilla koneidentiteeteillä ei ole kumpaakaan. Arvioikaa nykytila, ei suunnitelmia.

#	Vaatimus	Kysymys	Arvio	Arviointiperusteet
1	**Todennettava identiteetti**	Pystyttekö luettelemaan jokaisen agentin ja palvelutunnuksen, jolla on pääsy järjestelmiinne – ja näkyykö lokista, mikä niistä toimi?		**Vihreä** Jokaisella agentilla on oma identiteetti identiteetinhallinnassa, ja loki nimeää agentin. **Punainen** Jaettuja palvelutunnuksia. Kukaan ei tiedä, montako koneidentiteettiä on.
2	**Rajattu valtuutus**	Onko kirjattu, kenen puolesta kukin agentti toimii ja mitä se saa tehdä – ja onko se vähemmän kuin kaikki, mihin sen tunnus yltää?		**Vihreä** Nimetty päämies ja rajattu, määräaikainen, peruttava valtuutus jokaiselle agentille. **Punainen** Perityt oikeudet: agentti voi kaiken, mihin sen käyttöönottaja, tunnus tai integraatiot pystyvät.
3	**Tunnusten elinkaari**	Onko jokaisella agentin tunnuksella alkamis- ja päättymispäivä sekä omistaja, joka vahvistaa, että sitä yhä tarvitaan?		**Vihreä** Tunnukset luodaan, vaihdetaan, vanhenevat ja perutaan automaattisesti, samoin kuin ihmisten tunnukset. **Punainen** Avaimet vaihdetaan, kun joku huomaa. Agentteja ei koskaan poisteta käytöstä.
4	**Kattava kirjausketju**	Jos valvoja kysyisi, mitä yksi agentti teki viime kuussa ja kenen puolesta, saisitteko eheyssuojatun lokin omasta lokivarastostanne?		**Vihreä** Jokainen agentin toimi kirjataan agentin toimena, sidottuna päämieheen, allekirjoitettuna, omaan lokivarastoonne. **Punainen** Loki näyttää vain tunnuksen. Ainoa tallenne on agenttialustan oma loki.
5	**Sääntöjen valvonta reaaliajassa**	Kun agentti tekee virheen konenopeudella, kuka pysäyttää sen, millä mekanismilla ja kuinka monessa minuutissa?		**Vihreä** Yksi toimenpide pysäyttää agentin heti, ja säännöt, kuten tehtävien eriyttäminen, pätevät jokaisella kutsulla. **Punainen** Ainoa valvonta on määräaikainen käyttöoikeuksien katselmointi, ja peruminen tarkoittaa tikettiä.

Arvioikaa jokainen kysymys vihreäksi, keltaiseksi tai punaiseksi. Keltainen: pätee osaan agenteista tai on vasta suunnitteilla. Punaista kohdassa 1 eivät muiden vihreät kumoa – ilman omaa identiteettiä mitään muuta ei voi valvoa.

Mitä tuloksella tehdään

Vähintään kolme punaista tai punainen kysymyksessä 1:

Tällä viikolla Inventoikaa jokainen koneidentiteetti: palvelutunnukset, API-avaimet, pääsytunnisteet, botit ja agentit. Jos kukaan ei osaa sanoa lukua, se on ensimmäinen havaintonne.

Tässä kuussa Käykää nykyiset agentit läpi samalla mitalla kuin ihmiset: sama identiteetinhallinta, elinkaari, kirjausketju ja säännöt. Uusille agenteille nimetty, sopimukseen perustuva ja lokitettu identiteetti alusta alkaen.

Tällä neljänneksellä Yksi yhteinen hallintamalli ihmisille ja koneille riskirekisteriin omistajan ja päivämäärän kanssa, NIS2- ja tekoälyasetusvelvoitteiden rinnalle.

EU:n tekoälyasetus (26 artikla) tekee käyttöönottajasta vastuullisen käyttämästään tekoälystä riippumatta siitä, kuka sen rakensi. Identiteettikerros on ainoa paikka, joka näkee agentin jokaisen toimen – siellä vastuu toteutuu.

Tervetuloa juttelemaan Trivoren osastolle – tai osoitteeseen trivore.com/outnumbered.