UUSIKAUPUNKI

SIEM-järjestelmän ja siihen liittyvän SOC-palvelun laajentaminen

Kaupunginhallitus 11.09.2023 § 243
1802/02.08.00/2023

Valmistelija: ICT-päällikkö Pauli Lehtonen
pauli.p.lehtonen(ät)uusikaupunki.fi

Uudenkaupungin kaupunki on käyttänyt neljä vuotta (kh hankintapäätös 21.10.2019 § 375) kyberhyökkäysten havainnointiin tarkoitettua Kuntien Tiera Oy:n kilpailuttamaa Security Information and Event Management eli SIEM-järjestelmää ja siihen liitettyä Security Operation Center eli SOC-palvelua. Käytännössä palvelu toimii siten, että SIEM-järjestelmä seuraa eri järjestelmistä, kuten palomuurista ja palvelimista, saatavia lokeja sekä hälyttää poikkeuksista. SOC-palvelun avulla hälytyksiä suodatetaan sekä tarvittaessa ilmoitetaan niistä kaupungin ICT-yksikölle jatkotoimenpiteitä varten. Kokemukset palvelusta ovat olleet hyviä ja sen avulla kaupunki on pystynyt kehittämään teknistä tietoturvallisuutta merkittävästi mm. parantamalla palomuurisäännöstöä. Lisäksi olemme pystyneet reagoimaan nopeasti sellaisiin tietoturvaongelmiin, joita ilman palvelua emme edes huomaisi.

Kuntien Tiera on kilpailuttanut SIEM/SOC-palvelun kesän aikana uudelleen ja palveluntarjoajana jatkaa Insta Group Oy. Kaupungin ja Tieran välinen toistaiseksi voimassa oleva sopimus jatkuu entisellään, mutta liitteet päivittyvät, sillä kilpailutuksen tuloksena hinnoitteluperiaatteet muuttuvat. Lisäksi yleisen kustannustason nousu nostaa palvelun hintaa. Toisaalta uusi peruspaketti sisältää enemmän palveluita kuin aiemmin ja enemmän kuin mitä kaupungilla tähän asti on ollut käytössä. Hyvinvointialueuudistuksen tuoman verkkorakenteen ja laitemäärän muutoksen myötä ICT-palveluilla oli jo keväällä tarkoitus lähteä laajentamaan SIEM/SOC-palvelua mm. työasemiin sekä Microsoft 365 ympäristöön, jotta SIEM/SOC-palvelun tehokkuutta saataisiin parannettua, mutta sote-järjestelmien hidas siirtyminen Varhalle siirsi laajentamista syksyyn. Nyt uuden hinnoittelun myötä em. lisäpalvelut kuuluvat peruspaketin kuukausimaksuun ja vanhana asiakkaana lisäkustannuksia aiheuttaa vain kertamaksu lisäpalveluiden käyttöönotoista.

Esittelijä: Kaupunginjohtaja Atso Vainio

Päätösehdotus: Kaupunginhallitus päättää
- hyväksyä Kuntien Tiera Oy:n kilpailuttaman Security Information and Event Management eli SIEM-järjestelmän ja siihen ~~liitettyvän~~ liitetyn (korjattu hallintolain 51 §:n mukaisesti kirjoitusvirheenä khall 11.9.2023) Security Operation Center eli SOC-palvelun hinnoitteluperiaatteiden muutokset ja,
- että SIEM/SOC-palvelu laajennetaan sisältämään työasemat, Microsoft 365 ympäristö sekä Incident Response -palvelu ja samalla

parannetaan olemassa olevaa palvelinten havainnointikykyä lisäpaketilla.

Kertamaksu lisäpalveluista on yhteensä 6790,50 € ja jatkuva kuukausimaksu 15 hälytyksellä, 30 lisenssillä sekä IR-palvelulla yhteensä 3445 €.

Sopimus on voimassa toistaiseksi. Irtisanomisaika on 6 kk.

Päätös: Ehdotus hyväksyttiin yksimielisesti.

_____