Tietopyyntö

Valtorin lokienhallinta- ja SIEM-ratkaisujen kilpailutus

Sisällysluettelo

1 Tausta ... 3
2 Hankinnan kohdeympäristön kuvaus ... 3
2.1 Valtori ... 3
2.2 Keskitetty lokienhallinta ... 4
2.3 Tietoturvatapahtumien hallintaratkaisu (SIEM) ... 4
3 Keskeiset vaatimukset ... 4
3.1 Yhteiset vaatimukset ... 4
3.2 Lokiratkaisun yleiset vaatimukset ... 5
3.3 SIEM-ratkaisun yleiset vaatimukset ... 5
4 Kysymykset ... 6
5 Aikataulu ... 6
6 Toimittajainfo ... 7

1 Tausta

Tämä on lokienhallintaa ja SIEM-ratkaisuja koskeva tietopyyntö, jonka tarkoituksena on käynnistää tekninen vuoropuhelu palveluntuottajien sekä järjestelmätoimittajien kanssa liittyen Valtorin lokienhallinta- ja SIEM-ratkaisun kilpailutukseen. Tämä tietopyyntö ei sido tilaajaa eikä toimittajia.

Vastauksen jättäminen ei edellytä kaikkiin kysymyksiin vastaamista. Vastauksia voidaan kuitenkin käyttää hankinnan vaatimusten, kriteerien ja hankintamenettelyn määrittämiseen.

Vastauksiin pyydetään sisällyttämään riittävästi tietoa ratkaisusta. Erityisesti palvelukuvaukset, tekniset kuvaukset sekä toimintaperiaatekuvaukset auttavat hankinnan valmistelua. Vastaukset voi antaa myös englanniksi.

Päätökset mahdollisen hankintaprosessin käynnistämisestä ja aikataulusta tehdään tietopyynnön vastausten läpikäynnin jälkeen.

Hankintamenettelyn mahdollisen neuvotteluvaiheen aikana tullaan ratkaisemaan, toteutetaanko lokienhallinta- ja SIEM-ratkaisu Valtorin omilla lisensseillä ja laitteistoilla vai tullaanko toteutus hankkimaan toimittajan tuottamana kokonaispalveluna. On mahdollista, että valittavassa ratkaisussa tullaan hyödyntämään molempia edellä mainittuja vaihtoehtoja.

2 Hankinnan kohdeympäristön kuvaus

2.1 Valtori

Hankintayksikkönä on Valtion tieto- ja viestintätekniikkakeskus Valtori (jäljempänä ”Valtori”), joka on aloittanut toimintansa 1.3.2014. Valtori tuottaa valtionhallinnon toimialariippumattomat ict-palvelut. Näillä tarkoitetaan palveluita, joiden tuottaminen tai järjestäminen ei vaadi merkittävää toimialakohtaista osaamista ja jotka perustuvat yleisesti käytettyihin laite- ja ohjelmistoratkaisuihin ja teknologioihin. Palvelujen ja ratkaisujen asiakaskohtainen variointi ei tee niistä toimialakohtaisia.

Valtorin asiakkaita ovat kaikki valtionhallinnon organisaatiot. Lisäksi asiakkaita voivat olla valtion liikelaitokset, muut julkisen hallinnon viranomaiset, julkisoikeudelliset laitokset, eduskunta ja valtion talousarvion ulkopuoliset rahastot ja julkista hallinto- tai palvelutehtävää hoitavat yritykset tai yhteisöt.

Valtori tuottaa keskitetysti valtionhallinnolle yhteiset tieto- ja viestintätekniikkapalvelut ja huolehtii keskitetysti niiden hankinnasta, toimivuudesta, ylläpidosta ja kehittämisestä. Palvelujen tuottamisessa Valtori yhdistää itse tuottamaansa ja markkinoilta hankittua palvelua ja sovittaa palvelut valtionhallinnolle soveltuviksi.

Valtorin tuottamat palvelut ja palveluiden asiakkaat on määritelty laissa valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (1226/2013) ja valtioneuvoston asetuksessa valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä (132/2014). Valtorin turvallisuusverkon palveluja tuottavan TUVE-yksikön toiminta on määritelty turvallisuusverkkolaissa (Laki julkisen hallinnon turvallisuusverkkotoiminnasta (10/2015).

Valtorin palveluksessa on noin 1 000 ICT-ammattilaista ja toimimme useilla paikkakunnilla ympäri maata. Tarkoitus on, että Valtorin toimintoja keskitetään valittaville paikkakunnille niin, että toimipisteiden määrä pienenee. Valtorin vastuulla on noin 92000 työaseman ja niihin liittyvien palveluin sekä n. 8900 palvelimen konesali- ja kapasiteettipalveluiden hoito.

2.2 Keskitetty lokienhallinta

Keskitetyllä lokienhallintaratkaisulla tarkoitetaan ympäristöä, johon voidaan tallentaa eri lähteistä ja useilta asiakkailta tulevia lokeja niiden lähteestä tai muodosta riippumatta. Lokeja käytetään Valtorin omassa tuotannossa ja asiakasorganisaatioissa.

Lokienhallintaa käytetään mm. audit/käyttölokien hallintaan ja teknisen lokin hallintaan. Keskitetyllä lokienhallinnalla pyritään täyttämään paremmin myös lainsäädännölliset velvoitteet mm. lokitietojen säilytyksen ja muuttumattomuuden suhteen.

2.3 Tietoturvatapahtumien hallintaratkaisu (SIEM)

SIEM-ympäristöllä (Security Information and Event Management) tarkoitetaan tässä yhteydessä keskitettyä tietoturvatapahtumien hallintaratkaisua.

Hankittava SIEM-kokonaisuus palvelee alkuvaiheessa ensisijaisesti Valtorin omaa tuotantotoimintaa (mm. tietoturvavalvomo), mutta palvelu tulee olla tarjottavissa asiakkaille.

3 Keskeiset vaatimukset

3.1 Yhteiset vaatimukset

Ratkaisutavasta riippumatta Valtorin tulee voida tuottaa ja myydä hankittavalla ratkaisukokonaisuudella tuotettua palvelua asiakkailleen, joita voivat olla kaikki valtion virastot ja laitokset.

Mahdollinen hankinta sisältää toimitusprojektin tai -projektit mukaan lukien käyttöönotot ja ylläpidon asiantuntijapalvelut sekä muut tarvittavat tuki- ja ylläpito- sekä koulutuspalvelut.

Ratkaisukokonaisuus tulee voida ottaa käyttöön osissa ja se tulee voida hajauttaa.

Ratkaisukokonaisuuden tulee olla turvallinen, toimintavarma ja siinä tulee ottaa huomioon tietosuojavaatimukset.

3.2 Lokiratkaisun yleiset vaatimukset

Ratkaisukokonaisuuden tulee olla kustannustehokas ja sen tulee kyetä käsittelemään monipuolisesti suuria lokimassoja. Myös suurten massojen pitkäaikainen säilyttäminen tulee huomioida.

Ratkaisuissa ei ole tarkoitus sitoutua yhteen teknologiaan, tuotteeseen tai tekniikkaan vaan sen tulee pystyä vastaanottamaan kaikkea lokitietoa lokitiedon lähteen rajoittamatta.

Ratkaisukokonaisuuden tulee olla skaalautuva kustannustehokkaasti.

Asiakasorganisaation tulee voida halutessaan ilman toimittajan vuorovaikutusta tehdä hakuja kerättyyn lokiaineistoon ja muodostaa siitä raportteja.

Ratkaisukokonaisuuden toteuttamiseen valittavien järjestelmien tulee olla yhdistettävissä toisiinsa. Jokaisen osan toteuttamiseen tulee valita tarkoitukseen parhaiten sopiva tuote siten, että kokonaisuus toimii luotettavasti. Olemassa olevat lokienhallintajärjestelmät tulee olla mahdollista liittää osaksi tätä kokonaisuutta.

Ratkaisuun kerätty lokitieto tulee voida ottaa järjestelmästä ulos siten, että se voidaan siirtää tarvittaessa helposti toiseen järjestelmään. Samoin järjestelmään tulee voida viedä sisään muista lokienhallintajärjestelmistä otettua lokitietoa massasiirtoina järjestelmien välillä.

3.3 SIEM-ratkaisun yleiset vaatimukset

Ratkaisun tulee tukea operatiivista toimintaa ja sen tulee olla yhteensopiva lokienhallintaratkaisun kanssa.

Lisäksi ratkaisun tulee kyetä

- käsitellä erityyppisiä lähdetietoja
- korreloida erilaisia tietoja
- rikastaa/jalostaa tietoa
- muodostaa erilaisia raportteja
- tuottaa tilannekuvaa
- automatisoida toimintoja
- tehdä hälytyksiä.

4 Kysymykset

- Onko yrityksellänne mahdollisuus tarjota palvelua tai tuotteita sekä loki- että SIEM-osuuteen?
- Onko yrityksellänne mahdollisuus tarjota ratkaisuja sekä Valtorin omilla lisensseillä ja laitteistoilla sekä kokonaispalveluna toteutettuna?
- Kuvatkaa ratkaisun yleisperiaate Valtorin omilla lisensseillä ja laitteistoilla toteutettuna. Kuvauksia voi olla useampia.
- Kuvatkaa ratkaisun yleisperiaate kokonaispalveluna toteutettuna. Kuvauksia voi olla useampia.
- Onko yrityksenne toteuttanut kuvaamianne ratkaisuja aikaisemmin Valtorin vaatimuksia vastaaviin tarpeisiin sekä ympäristöihin?
- Pyydämme liittämään mukaan tarkentavia kuvauksia ottaen huomioon liike- ja ammattisalaisuuden. Voitte halutessanne toimittaa hankinnan suunnittelua tukevia mahdollisimman kattavia teknisiä kuvauksia, palvelukuvauksia ja muita hankinnan kohdetta kuvaavia dokumentteja.
- Onko teillä kommentteja tai yleishavaintoja, jotka Valtorin olisi hyvä ottaa huomioon suunnitellussa hankinnassa? Onko edellä esitetyssä kokonaisuudessa joitain osia, joiden tuottaminen ei onnistu tai olisi mielestänne liian kallista tai hankalaa?

5 Aikataulu

Tähän tietopyyntöön pyydetään vastauksia 13.2.2017 klo 12.00 mennessä osoitteeseen Kilpailutukset@Valtori.fi otsikolla ”keskitetty lokienhallinta- ja SIEM- tietopyyntö”. Toimittajien niin halutessa, vastaukset voidaan toimittaa myös Cloudiaan pelkästään. Jos vastaukset sisältävät luottamuksellista tietoa, pyydämme merkitsemään asiakirjat luottamuksellisiksi.

Vaihtoehtoisesti voitte lähettää vastauksenne turvasähköpostilla kirjaamon turvasähköpostiosoitteeseen osoitteessa https://turvaposti.valtori.fi/, turvapostin vastaanottajaksi merkitään kirjaamo@valtori.fi. Merkitkää tunnukseksi ”keskitetty lokienhallinta- ja SIEM – tietopyyntö”.

6 Toimittajainfo

Valtori kutsuu toimittajat keskustelemaan tästä tietopyynnöstä ja suunnitteilla olevasta hankinnasta Valtorin tiloihin 2.2.2017 klo 15-16 osoitteeseen Lintulahdenkuja 4, Helsinki. Pyydämme ilmoittautumaan viimeistään 30.1.2017 osoitteeseen Kilpailutukset@Valtori.fi.

Valtori toivoo, että tilaisuuteen osallistuisi enintään kaksi henkilöä toimittajaa kohti.