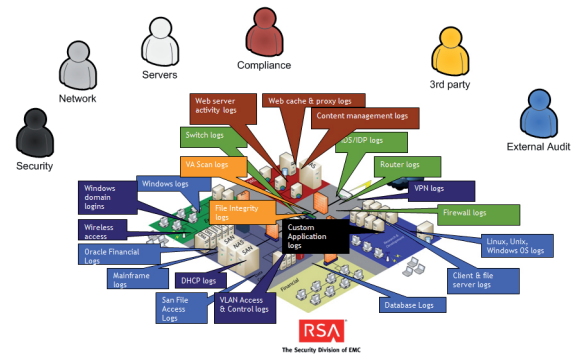


## Tiedätkö mitä tietoverkossasi ja palveluissasi tapahtuu?

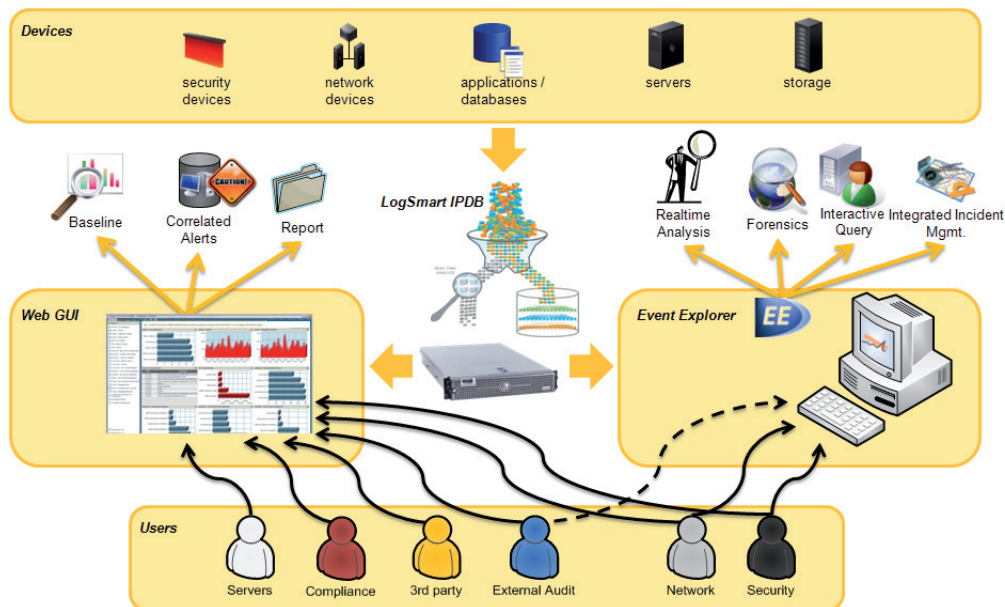
*Loki- ja tapahtumatietojen keskittäminen yhteen paikkaan tuo monia hyötyjä. Oikeanlaisen järjestelmän avulla lokit saadaan muuttumattomana turvallisesti säilöön ja niitä päästään käsittelemään tehokkaasti sekä monipuolisesti. Security Information and Event -järjestelmä (SIEM) antaa työkalut erilaisten tapahtumien visualisointiin ja ymmärtämiseen. Järjestelmä antaa oikein käytettynä järjestelmäriippumatonta tietoa tietoverkon historiapohjaisesta tai reaaliaikaisesta tilanteesta, oli kyseessä sitten tietoturvaan, tietoverkkoon, käyttöjärjestelmiin, sovelluksiin tai ongelma- ja vikatilanteisiin liittyvät tapahtumat.*

### Mitä lokitiedoilla pitäisi tehdä?

Lokitietojen avulla pystytään valvomaan tietoturvaliikkeen mukaista järjestelmien, verkkojen ja palvelujen käyttöä, raportoimaan selkeästi erilaisista tapahtumista, ratkaisemaan ongelmatilanteita, selvittämään väärinkäytöksiä ja tekemään hälytyksiä mm. tietoturvaliikkeen vastaisesta käytöstä, vikatilanteista, suorituskyky- tai kapasiteettiongelmistä. Vaikka lokitietojen ja tapahtumien keskittäminen onkin monelle tuttua, se ei ole aivan yksiselitteistä, sillä lokitiedot on pystyttävä keräämään kaikista eri valmistajien loki- ja tapahtumalähteistä. Vastaanottamisen lisäksi tulee pystyä tunnistamaan ja analysoimaan kerättyjä lokitietoja automaattisesti. Järjestelmästä on löydettävä valmiita raportteja ja työkalut lokien käsitteilyyn myös räätälöidyistä sovelluksista. Mitä laajempi tuki ja monipuolisemmat työkalut, sitä helpompi ja nopeampi on käyttöönotto.

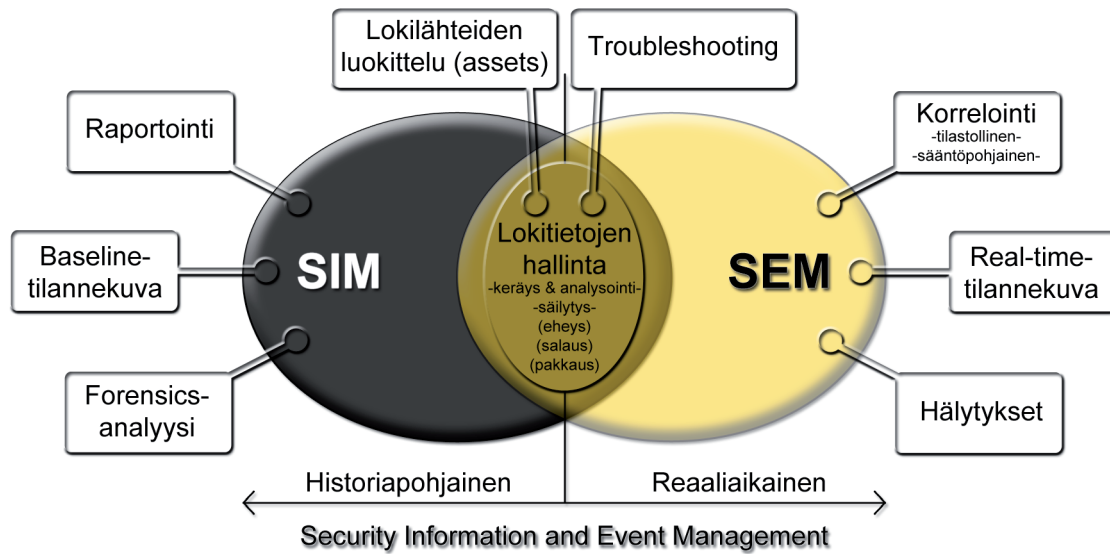


Edellä mainittujen ja monien muiden vastaavanlaisten teknisten yksityiskohtien lisäksi tarvitaan systemaattista suunnittelua siitä, mitä ratkaisulla halutaan saavuttaa. Tietoturvainformaation ja -tapahtumien hallinta eli englanniksi Security Information and Event Management (SIEM) sisältää tietoturvamielessä osakokonaisuuksia, joiden hyödyntäminen vaatii tarkkaa suunnittelua ja vaiheistusta. Onnistuneeseen kokonaisuuteen päästään, kun suunnitteluun sitoutuvat sekä toimittaja että asiakas.



**SIEM-järjestelmä järjestää yksittäiset lokit ymmärrettävään muotoon tapahtumakategorioiden ja raportointitaulujen avulla. Käyttötarpeesta riippuen tietoa käsitellään RSA enVision SIEM-järjestelmässä Web GUI:n tai dynaamisemman Event Explorerin kautta.**





## SIEM ja sen toiminnallisuudet

Security Information and Event Management -termi on jaettava kahteen osaan: Security Information Management (SIM) ja Security Event Management (SEM). SIM-toiminnallisuudet perustuvat historiapohjaisen tiedon käyttämiseen, kun SEM-toiminnallisuuksien painoalue on reaaliaikaisissa tapahtumissa. Molemmissa alueissa toiminnallisuudet perustuvat tehokkaaseen lokien hallintaan, analysointiin ja säilytykseen. Yhdistävinä asioina ovat myös lokilähteiden kriittisyysluokittelu sekä ongelmatilanteiden ratkaiseminen (troubleshooting), jota voidaan luonnollisesti tehdä sekä historiapohjaisten että reaaliaikaisten tapahtumien perusteella.

**SIM:in** keskeisimpiä toiminnallisuuksia ovat raportointi, baseline-tilannekuvan muodostaminen ja forensics-analyysi. Raportoinnin tarkoituksena on tuottaa lokeista informatiivisia raportteja, joiden perusteella nähdään, mitä verkossa on tapahtunut ja mitä tietoteknisiä tai tietoturvaan liittyviä parannuksia verkkoon olisi syytä tehdä. Baseline-tilannekuva muodostuu ajansaatossa ja se kuvaa verkon eri systeemikomponenttien normaalitilaa. Baseline-tilannekuvaa voidaan hyödyntää SEM:in yhteydessä, kun halutaan tehdä esimerkiksi hälytyksiä poikkeavuuksista. Forensics-analyysia tarvitaan silloin, kun jotain ongelmatilannetta tai tietoturvaloukkausta halutaan tutkia tarkemmin joltain kuluneelta ajanjaksolta.

**SEM:in** avulla saavutetaan reaaliaikainen tilannekuva verkon ja sen palveluiden tapahtumista. Tarkoituksena on pääasiassa tehdä hälytyksiä erilaisista tietoturvatapahtumista, mutta samalla voidaan valvoa esimerkiksi erilaisten palveluiden resursseja tai tietoverkon palveluiden vikatilanteita. Tarkkoihin hälytyksiin päästään tapahtumien korreloinnin avulla, jota voidaan tehdä sääntöpohjaisesti tai tilastollisesti.

Sääntöpohjaisessa tavassa hälytys voi nojautua johonkin tiettyyn tapahtumaan. Esimerkiksi IDS-järjestelmä on havainnut hyökkäyksen ja lähettänyt sen SIEM-järjestelmälle. SIEM-järjestelmällä voi olla tiedossa kohteena olevan järjestelmän haavoittuvuudet ja määritelty riskitaso. Korreloimalla hyökkäystietoa tunnettuihin haavoittuvuuksiin ja riskitasoon saavutetaan huomattavasti tarkempi hälytys, kuin pelkästä IDS-järjestelmästä. Toisaalta sääntöpohjaisessa korreloinnissa voidaan tehdä hälytys esimerkiksi liiallisista kirjautumisyriyksistä, tiedostopalvelimen levytilan loppumisesta jne. Tilastollisella korreloinnilla verrataan baseline-tilannekuvaa reaaliajan tilannekuvaan ja tehdään mahdollisista poikkeavuuksista haluttuja hälytyksiä.

SEM on SIEM-projektin haasteellisin ratkaisualue ja useasti SEM-toiminnallisuudet otetaan käyttöön vasta onnistuneen SIM-toteutuksen jälkeen. Projektia haasteellisempi osuus voi olla myös siihen liittyvien prosessien kehittäminen. Ongelmien tai uhkien havaitseminen onnistuu teknisesti, mutta niihin reagoiminen ja niiden korjaus voi olla huomattavasti hankalampaa.

