Lokien keräys ja käyttö

Ohje lokitietojen tallentamiseen ja hyödyntämiseen

Ohje 4/2016

Viestintävirasto

Sisältö

Viestintävirasto julkaisi maaliskuussa 2016 sarjan lokitus-aiheisia teemakirjoituksia. Lokitus tarkoittaa lokitietojen tallennusta ja hyödyntämistä. Lokitietoa tarvitaan selvittämään, mitä, miksi ja milloin jotakin tapahtui. Kirjoitukset käsittelivät, millaisissa järjestelmissä erilaisia lokeja käytetään, mitä ja miten lokeja voi käyttää hyödykseen ja mitä lainsäädäntöä ja määräyksiä on huomioitava lokeja määriteltäessä. Kirjoitukset on koottu tähän ohjeeseen.

1 Lokitiedot tietoturvallisuuden tukena

Tietokoneet, puhelimet, reitittimet ja operaattorit keräävät säännöllisesti lokitietoja käyttämistämme laitteista. Lokien avulla asiat varmistetaan, virheet korjataan ja tietomurrot havaitaan. Huolehdi siitä, että järjestelmiesi loki on kunnossa.

1.1 Loki havainnoi tapahtumia

Loki tarkoittaa aikajärjestyksessä kirjattua tallennetta tapahtumista ja niiden aiheuttajista. Tapahtumat ja muutokset tietojärjestelmissä, sovelluksissa, tietoverkoissa ja tietosisällöissä kirjataan lokiin, eli lokitetaan.

Lokitietojen tallentamisen historia alkoi merenkulusta, jossa laivan lokikirjaan kirjoitettiin säännöllisin aikavälein muun muassa aluksen nopeus ja suunta sekä muita merkittäviä tapahtumia. Pitkillä merimatkoilla laivan kapteeni saattoi pitää päiväkirjaa, kapteenin lokia. Nykyään myös tietojärjestelmät dokumentoivat tapahtumiaan kirjaamalla lokeihin sekä rutiinit että poikkeamat.

Lokia syntyy koko ajan kaikkialla. Tietokoneesi kerää käyttölokia, langattoman verkon tukiasema ja lankaverkon reititin tallentavat tapahtumalokia, puhelimesi operaattori kirjaa viestintälokia, jokapäiväiset ohjelmistosi pääsynvalvontalokia, virhelokia ja niin edelleen.

1.2 Miksi lokitetaan?

Lokitiedot kertovat, mitä, miksi ja milloin jotakin tapahtui. Tiedoilla selvitetään virhetilanteita, tai varmistetaan että virheitä ei ole syntynyt ja käsitelty tieto on oikeaa. Ilman asianmukaista lokitietoa virheiden syitä on mahdoton selvittää ja niiden korjaaminen hyvin vaikeaa. Usein järjestelmiltä vaaditaan tiedon kiistämättömyyttä ja autenttisuutta, minkä todistaminen vaatii monipuolista lokitusta.

Lokitietoja säilytetään riittävän pitkään, jotta niihin voidaan tarpeen vaatiessa palata pitkänkin ajan kuluttua. Tietoturvapoikkeamien havainnoimiseksi lokeja voidaan analysoida joko reaaliaikaisesti tai jälkeenpäin.

1.3 Lokia käytetään tapahtumien selvittämiseen

Lokia ei kerätä vain muodon vuoksi, vaan tarpeeseen. Maksuliikenteestä on tärkeää voida selvittää myös jälkeenpäin maksajat, maksun saajat ja summat, jotta virhetilanteista voidaan toipua hallitusti. Tietoturvan ylläpidossa lokitietojen rooli on hyvin keskeinen. Viestintälokin analysointi selvittää tietoliikenteen poikkeamat, pääsynvalvontaloki selvittää järjestelmän murtautumisen kulun ja muutosloki auttaa korjaamaan murtaudutun sivuston sisällöt.

1.4 Sopiva loki joka lähtöön

Lokeja on monen tyyppisiä ja jokaisella on oma muotonsa, käyttötarkoituksensa ja käyttötapansa.

Ylläpitolokilla ylläpidetään tietoa järjestelmän toimintaan tehdyistä muutoksista ja järjestelmän käyttöoikeuksien muutoksista sekä hallitaan virhetilanteita. Tämänkaltainen loki on hyvin tarpeellinen versionhallinnassa ja toimintaympäristön kokonaisarkkitehtuurin seurannassa.

Käyttöloki eli **tapahtumaloki** lienee tavallisin ja välttämättömin lokimuoto. Se rekisteröi käyttäjien sisään- ja uloskirjautumisista ja muista normaaleista

järjestelmän suorittamista prosesseista. Järjestelmän moduulit jättävät jäljen käyttölokiin kutsuessaan toisia moduuleita. Tulostustapahtumista ja tietosisällön lukemisesta tietokannasta kirjataan merkintä käyttölokiin.

Muutoslokiin on kirjattava merkinnät tietojen lisäyksistä, poistoista ja muutoksista. Muuttuneen tiedon alkuperä on syytä selvitä lokimerkinnöistä, jotta sen oikeellisuus voidaan tarvittaessa jäljittää ja varmistaa.

Virheloki on erityisen tarpeellinen ongelmatilanteiden selvittämisessä. Kun virheen syy kirjataan lokiin mahdollisimman tarkasti, sen aiheuttaja on myös helpompi korjata.

Myös muita yleisiä lokimuotoja käytetään yleisesti. **Viestintäloki** voi sisältää tiedot kulkeneesta viestinnästä: viestin alkuperän, päätepisteen ja muita tietoja kuten ajankohdan, määrän, yksikäsitteisen tunnisteen ja tilan. Teletunnistetiedot ovat tällaisia viestintälokitietoja. Yleisimmät sähköpostipalvelimet on asetettu kirjaamaan viestintälokia.

Haltijaloki kertoo, kenelle jokin nettiosoite, tai puhelinnumero, tai verkkodomain, tai autovuokraamon auto on kuulunut tiettynä ajanhetkenä. Haltijatieto voidaan yhdistää suoraan henkilöön tai organisaatioon tai järjestelmään.

Pääsynvalvontaloki kertoo sisään- ja uloskirjautumisista, sekä onnistuneista että epäonnistuneista. Kulunvalvontaloki on samaa tyyppiä, vaikka usein vain viitteellinen. Jos samalla ovenavauksella pääsee kulkemaan useampi, kulunvalvonta ei tuota täydellistä pääsynvalvontalokia. Pääsynvalvontalokia analysoimalla on helppo raportoida tietoturvapoikkeamista: onko yritetty murtaa salasanoja tai kirjautua jo vanhentuneilla käyttäjätunnuksilla.

Pääsynvalvontalokien avulla voi myös seurata organisaation käyttölupien pysymistä ajan tasalla. Käyttölupien muutokset eivät aina seuraa riittävän nopeasti tehtävästä toiseen siirtyneitä käyttäjiä. Tarpeettomat oikeudet on aina syytä poistaa.

1.5 Lisätietoja

- VAHTI-lokiohje

- Lokiteeman Tietoturva nyt! -artikkelit maaliskuussa 2016 Viestintäviraston teemana:

[Teema] Lokitiedot tietoturvallisuuden tukena (TTN 4.3.2016)
[Teema] Loki on ylläpidon tärkein turvallisuustyökalu (TTN 10.3.2016)
[Teema] Vieraskynä: SIEM lokitiedon hyödyntämisessä (TTN 15.3.2016)
[Teema] Lokien käsittelyn on perustuttava lakiin (TTN 22.3.2016)
[Teema] Loki – tietoturvan väsymätön kirjuri (TTN 31.3.2016)

2 Loki on ylläpidon tärkein turvallisuustyökalu

Mitä lokissa pitää ainakin olla mukana ja paljonko lokitietoa on tarpeeksi? Mitä riskejä vääränlainen lokitus aiheuttaa?

Kun ongelmat kasaantuvat, lokitieto on korvaamatonta. Hyvä lokiympäristö on erotettu muusta järjestelmästä, sen muokkaaminen on estetty ja sen pääsynvalvonta on tarkkaan säädetty vastaamaan tarvetta. Vain riittävän kattava lokitus tarjoaa parhaan työkalun järjestelmän ylläpitoon.

2.1 Miten lokitetaan tarpeeksi?

Järjestelmä on murrettu, joku on vienyt tiedot, sivusto on sotkettu ja asiakkaille on ohjattu haittaohjelmia. Vain kunnollinen loki auttaa kertomaan, miten ongelmat saadaan selvitettyä ja katastrofit korjattua.

Jokaisen järjestelmän pitäisi kirjata lokitiedot omista tapahtumistaan. Sekä käyttäjien toimenpiteet että automaattiset tapahtumat on tärkeää kirjata talteen. Hyvin rakennettu lokiympäristö on muusta järjestelmästä erillään oleva tietokanta, jonka eheys on varmistettu niin, ettei sitä voi jälkeenpäin muokata. Myös lokitietojen katselu ja käsittely on syytä lokittaa erikseen.

Lokista tulee käyttökelpoinen vain, jos siinä on riittävästi tietoa sen käyttötarkoitukseen. Käyttökelpoisen lokitiedon pitäisi sisältää ainakin nämä määritteet:

- Aikaleima (milloin tapahtuma oli?)
- Tapahtuma (mitä tehtiin tai yritettiin tehdä?)
- Toimija (kuka tai mikä teki?)
- Käyttöoikeus (millä valtuuksilla tai oikeuksilla tapahtuma tehtiin?)
- Tapahtuman lähde (mistä tehtiin, mistä muutostieto on peräisin?)
- Tapahtuman kohde (mihin tietoon tai järjestelmään toiminta kohdistui?)
- Tapahtuman tila (onnistui / ei onnistunut / epäonnistumisen syy)

2.2 Mitoita lokitus sopivaksi

Lokitietojen sopiva tallennustahti löytyy helpoiten kokeilemalla. Harva asiantuntija osaa suoralta kädeltä sanoa joka järjestelmästä, paljonko lokitietoja pitäisi tallentaa. Aloita varovasti ja lisää sitten tiedonkeruun yksityiskohtaisuutta tarpeen mukaan. Jos käyttöönotossa säätää lokituksen liian raskaaksi, se tukkii järjestelmän nopeasti ja hyödyllistä tietoa on vaikea seuloa kaiken massan alta.

Lokien säilytysaikaa kannattaa säätää mieluummin vähintään riittävän pitkäksi kuin liian lyhyeksi. Lokien riittävä säilytysaika vaihtelee suojattavan kohteen mukaan yleensä kuuden ja 24 kuukauden välillä. Tarvittavan lokitilan määrää voi yrittää arvioida esimerkiksi kuukauden keskimääräisen lokikertymän perusteella. Tilaa on hyvä varata puskuriksi enemmänkin, sillä poikkeavat tilanteet ja jotkin hyökkäystyypit voivat kasvattaa lokikertymää.

2.3 Arkistointi ja poisto

Arkistoimalla lokitietoja varmistetaan mahdollisuus palata vanhempiinkin havaintoihin, joita ei esim. tilankäyttösyistä ole mahdollista pitää aktiivisessa käytössä olevassa lokissa. Lokitiedoilla on yleensä elinkaari, jonka lopussa tiedoille ei enää ole käyttöä eikä niiden säilyttäminen ole tarpeen. Lokitietojen poistamiselle tulisi myös olla menettely.

2.4 Vastuut lokien käsittelyssä

Lokien käsittelystä vastaavat ensisijaisesti tehtävään nimetyt pääkäyttäjät. Seurattavuuden varmistamiseksi yksittäisillä pääkäyttäjillä ei tulisi olla muokkausoikeuksia keskitettyyn lokienhallintajärjestelmään.

Lokiseloste määrää, mihin tarkoitukseen lokitietoa kerätään ja mihin lokitietoa saa käyttää. Jokaiselle kerättävälle lokitiedolle on oltava peruste. Lokien turvallisuutta ja asianmukaisuutta on auditoitava säännöllisesti. Ylläpitäjät seuraavat heille tarpeellisia lokeja, tietoturvavastaavat seuraavat tietoturvallisuuteen

liittyviä lokeja ja viime kädessä lokitiedosta vastaa organisaation ylin johto.

2.5 Väärälle paikalle kirjattu salasana jää näkyviin

Kirjautumislokiin tallennetaan yleensä sekä onnistuneet että epäonnistuneet kirjautumisyritykset. Kirjautumisen tunnistetietoina tallennetaan esimerkiksi käyttäjätunnus, ajankohta ja osoite, josta kirjautumisyritys tehtiin. Myös vääristä kirjautumisyrityksistä jää merkintä, jonka voi lukea lokista. Kuinka usein olet vahingossa kirjoittanut käyttäjätunnuksen paikalle salasanasi ja painanut enteriä? Se on nyt tallessa lokissa, jonka ylläpitäjä voi lukea selväkielisenä. Kannattaa aina vaihtaa salasana, jonka on lipsauttanut näkyvälle paikalle.

2.6 Mitä huonosta tai väärästä lokituksesta voi seurata?

Loki voi tietosisältönsä vuoksi olla osa henkilörekisteriä, jolloin siitä on mainittava myös järjestelmän rekisteriselosteessa. Liian yksityiskohtainen tapahtumaseuranta yhdistettynä henkilöiden identiteetteihin saattaa rikkoa yksilön tietosuojaa.

Vältä tallentamasta lokiin näitä tietoja:

- henkilötunnukset
- henkilötietolain määrittelemiä arkaluonteisia henkilötietoja
- luottokorttinumeroita
- salasanoja (ei edes tiivistemuotoisia)
- järjestelmien välisiä käyttöavaimia ja salaisuuksia
- valtuutustietoja
- henkilöiden välisen viestiliikenteen sisältöä.

Lokien käsittely edellyttää tarkoin harkittua pääsynvalvontaa. Lokit ja niiden kirjauspalvelut voi suojata asiattomalta käytöltä parhaiten muusta tuotantoympäristöstä erillisellä lokiympäristöllä, jonka eheys eli muuttumattomuus on varmistettu.

Erityisesti tulee huolehtia järjestelmän erottelusta muusta ympäristöstä siten, että mahdollinen tietoturvaloukkaus ei pääse vaikuttamaan lokitapahtumien eheyteen. Myös lokitiedot on syytä varmuuskopioida ja niiden käsittelystä kirjata lokimerkintöjä sekä asiattomista muokkausyrityksistä säätää hälytykset.

2.7 Mihin lokia ei saa käyttää?

Tarkimmillaan lokiin voi tallentua selkeä tilannekuva jonkin ympäristön tapahtumista. Loki voi sisältää henkilötietoja, jotka on helppo yhdistää järjestelmän tapahtumiin. Lokeista on luvallista selvittää, kuka on virkatehtävänään avannut joitakin tiettyjä luottamuksellisia tietoja. Sen sijaan lokeista ei saa etsiä, ketkä ovat ladanneet lomakepankista irtisanoutumiskaavakkeen ja selanneet verkossa avoimia työpaikkoja, josta voitaisiin päätellä henkilön aikeita vaihtaa työnantajaa.

2.8 Lisätietoja

KATAKRI 2015 - Tietoturvallisuuden auritointityökalu viranomaisille.

3 Lokien käsittelyn on perustuttava lakiin

Laki asettaa vaatimuksia lokin sisällölle, säilytysajalle, lokeissa olevan tiedon eheyden varmistamiselle ja lokin käyttötarkoitukselle.

Lokeja tarvitaan esimerkiksi tietojärjestelmien toimivuuden takaamiseen, järjestelmien käytön tilastointiin sekä tietoturvasta huolehtimiseen. Lokin keräämisen sekä käsittelyn on perustuttava lakiin.

Lokeja on erilaisia, siksi niiden käsittelytapa ja -oikeus riippuvat siitä, millaista tietoa loki sisältää ja mihin tarkoitukseen lokia on alun perin kerätty.

Lakiin perustuvat lokien vaatimukset liittyvät sisältöön, säilytysaikaan, lokeissa olevan tiedon eheyden varmistamiseen sekä lokitiedon käyttötarkoituksiin. Lisäksi lokien käsittelyssä on otettava huomioon organisaation sisäiset ohjeet, jos sellaisia on annettu.

3.1 Henkilötiedot tekevät lokista henkilörekisterin

Jos lokitiedot sisältävät henkilötietoja, muodostuu lokista henkilörekisteri. Henkilötiedolla tarkoitetaan kaikenlaisia merkintöjä, jotka voidaan tunnistaa luonnollista henkilöä koskevaksi. Tällöin on huomioitava etenkin henkilötietolain asettamat velvoitteet ja tuotettava rekisteriseloste. Lokitietoon liitettyinä henkilötiedoiksi katsotaan esimerkiksi nimi tai sähköpostiosoite.

Jos kyseessä on sähköisen viestinnän välitystietoja sisältävän lokin käsittely, lokitietoja on käsiteltävä tietoyhteiskuntakaaren 17. luvun mukaan. Välitystietoja ovat esimerkiksi tiedot sähköpostiviestin lähettäjästä ja vastaanottajasta, verkko-osoite, tiedot yhteyden kestosta, reitityksestä, ajankohdasta sekä siirretyn tiedon määrästä.

Jos lokia tai sitä tuottavaa teknistä järjestelmää on tarkoitus käyttää henkilöstön valvontaan esimerkiksi yrityssalaisuuksien suojaamiseksi tai väärinkäytöstapausten selvittämiseksi, lokin käytössä sovelletaan tietoyhteiskuntakaaren 18. luvun niin sanottuja Lex Nokia -pykäliä. Tällöin menettelystä on tiedotettava myös käyttäjille. Lisäksi työnantajan on järjestettävä yhteistoimintamenettely.

Lokien hallinta on rajattava niin, että kaikki lokit tai edes yksittäisen lokin tiedot eivät ole kaikkien saatavilla. Käsittelyoikeuksia tulisi siis rajata esimerkiksi henkilön työtehtäviin perustuvan tietotarpeen perusteella. Tämä tarpeellisuusvaatimus, niin sanottu "need to know basis", on kirjattu sekä henkilötietolakiin että tietoyhteiskuntakaareen.

3.2 Lokittajan muistilista

Lokin oikeaoppinen rakentaminen ja lokitietojen käsittely vaatii huolellista suunnittelua, selkeätä prosessia ja ohjeita. Tässä pieni lokittajan muistilista, jonka avulla lokiprojektin pitäisi onnistua:

- Mieti, mikä lokituksen tarkoitus on.
- Ovatko lokiin tallennettavat tiedot tarpeellisia käyttötarkoituksen kannalta?
- Muista lainsäädännön velvoitteet erityyppisille lokeille.
- Käsittele ja poista lokitietoja ennalta määriteltyjen järjestelmien ja toimintatapojen mukaisesti.
- Määrittele käyttöoikeudet tietotarpeen perusteella.
- Rekisteröityjen ja ylläpidon tietosuojasta ja oikeusturvasta on huolehdittava.
- Informoi käyttäjiä riittävästi etenkin, jos kyse on teknisestä valvonnasta. Muista myös YT-menettely.

3.3 Lokeja koskeva lainsäädäntö

Lokien käsittelyvaatimukset perustuvat muun muassa seuraavaan säädäntöön:

- Henkilötietolaki (22.4.1999/523)
- Laki yksityisyyden suojasta työelämässä (13.8.2004/759) ("työelämän tietosuojalaki")
- Tietoyhteiskuntakaari (7.11.2014/917)

Lisäksi julkisyhteisöihin soveltuvat vielä seuraavat:

- Laki viranomaisten toiminnan julkisuudesta (21.5.1999/621)
- Julkisuusasetus (12.11.1999/1030)
- Arkistolaki (23.9.1994/831)
- Asetus Tietoturvallisuudesta valtionhallinnossa (1.7.2010/681)
- Pakkokeinolaki (22.7.2011/806)
- Poliisilaki (22.7.2011/872)

3.4 Lisätietoja

Tietosuojavaltuutetun toimiston ohje Henkilötietolain mukaisesta ilmoitusvelvollisuudesta

- Ohjeita rekisteri-ilmoituksen tekemiseksi ja täsmennyksiä siitä, mikä voi olla henkilötieto.

4 Lokitus ja SIEM

4.1 Mikä ihmeen SIEM?

SIEM (*Security Information and Event Management*) on nopeasti noussut tietoturva-alan kuumaksi puheenaiheeksi. Mistä koko hype aiheen ympärillä on syntynyt ja mitä SIEM:llä tarkoitetaan?

Useimmiten SIEM:stä puhutaan tietoturvatuotteena, joka yhdistää muiden olemassa olevien järjestelmien tuottamaa informaatiota yhteen. Tämä ajatusmaailma ei kuitenkaan tuota niin suurta lisäarvoa SIEM:n käyttöönottajalle, kuin mitä SIEM parhammillaan voi tarjota. Lokienhallintaa ja SIEM:iä pitäisi ensisijaisesti ajatella prosessina tai tietoturvan hallinnan tapana, joka mahdollistaa tiedon keruun useista toisistaan suoraan riippumattomista järjestelmistä. Kerätty tieto joko tallennetaan tai käsitellään keskitetyssä paikassa, ja näin luodaan mahdollisuus havaita useista pienistä palasista koostuvia suurempia tapahtumia. SIEM:n suurin vahvuus piilee juuri mahdollisuudessa näyttää ja korreloida tietoa keskitetyssä pisteessä.

Suurin harhaluulo SIEM:stä on oletus valmiista tuotteesta, joka tuottaa lisäarvoa pelkästään olemassaolollaan. Tällä saavutetaan kuitenkin harvoin merkittävää lisäarvoa tai tilannekuvan kehittymistä.

4.2 Keskitetyn lokienhallinnan käyttöönotto

Tärkeintä on ensin määritellä lokienhallintapolitiikka. Mitä lokitetaan, miten lokitetaan ja erityisesti mitä kerätyllä lokilla tehdään. Lokienhallinnan eräs keskeisimpiä ongelmia on tapahtumien valtava määrä. Se johtaa hyvin nopeasti tilanteeseen, että lokienhallintajärjestelmien ylläpitäjät eivät enää kykene tehokkaasti etsimään tietoa lokimassasta. Keskitettyä lokienhallintaa käyttöönotettaessa on syytä määritellä tarkkaan, miksi tämä toimenpide tehdään.

Keskitetty lokienhallintajärjestelmä voidaan ottaa käyttöön esimerkiksi jonkin vaatimusmäärittelyn sanelemana. Tällöin siitä ei kannata yrittää rakentaa turhan raskasta järjestelmää, jos organisaatio ei ole kokonaisuudessaan valmis siirtymään SIEM-prosessiin. Lisäksi on syytä varoa markkinointimateriaalia, jossa SIEM-tuotteen käyttöönoton jälkeen organisaatio täyttäisi heti tietyn vaatimusmäärittelyn. Tämä on käytännössä aina vain markkinointilause, eikä siihen tule tällaisenaan uskoa. Keskitettyä lokienhallintaa ja erityisesti SIEM:iä käyttöönotettaessa on maltti usein valttia. Käytännössä tämä tarkoittaa seurattavien lokilähteiden asteittaista lisäämistä ja omien toimintatapojen samanaikaista kehittämistä resurssien puitteissa. Usein ensimmäinen keino ennen SIEM-järjestelmän hankintaa voi olla yksittäisen lokipalvelimen pystyttäminen ja komentorivipohjaisten komentorivihakujen kokeilu.

4.3 Lokienhallinta käytännössä

Keskitetyn lokienhallinnan ja SIEM:in ei pidä luulla mullistavan organisaatioiden tietoturvaa sellaisenaan. Vaikka organisaatiossa käytettäisiin järjestelmään resursseja (hankinta, asennus ja lähdejärjestelmien liittäminen), ei pidä odottaa SIEM-järjestelmän tuottavan yksinään hälytyksiä tai havaintoja. On totta, että varsinkin kaupallisest SIEM-tuotteet sisältävät valmiita tunnistetietoja, joiden avulla voidaan haitallisia tapahtumia havainta. Jokaisen organisaation IT-ympäristö on yksilöllinen, eivätkä valmiit yleiset tunnisteet riitä tuomaan merkittävää lisäarvoa Antivirus-järjestelmien lisäksi. Toisessa ympäristössä tietty tapahtumasarja voi näyttää hyökkäykseltä, kun taas toisessa se on osa normaalia tapahtumankulkua.

Lokienhallintajärjestelmän suurin vahvuus on tapahtumien korrelointi keskitetyssä pisteessä. Järjestelmästä ei kannata rakentaa vain johdon työkalua, josta muutama henkilö voi käydä katsomassa viimeaikaisia tapahtumia. Lokienhallintajärjestelmä tulisi ottaa organisaation tietoturvaryhmän, verkkoylläpitäjien tai vastaavien ryhmien aktiiviseksi työkaluksi, joka sekä tehostaa näiden työskentelyä että mahdollistaa tietoturvapoikkeamien havainnoinnin.

Lokienhallinnan ja SIEM-prosessin keskeinen tavoite on pyrkiä saada koko IT-ympäristö toimimaan eheästi SIEM-järjestelmän ympärillä. Monissa organisaatioissa se asettaa merkittäviä käytännön haasteita. Hyvänä esimerkkinä tästä voidaan pitää palomuurin droplokia, jota generoituu huomattavia määriä väärin konfiguroiduista palveluista. Liian suuri väärien positiivisten hälytysten lokitulva ajaa SIEM-järjestelmän tilanteeseen, että hälytykset joudutaan mahdollisesti poistamaan käytöstä. Jotta SIEM-järjestelmistä saadaan niiden paras hyöty irti, tulee monitoroitava osa IT-ympäristöstä asettaa sellaiseen tilaan, että SIEM-järjestelmän korrelaatiosääntöjä voidaan tehokkaasti hyödyntää.

4.4 Suosituksia käytännön toimenpiteiksi

Alla on lyhyesti Kyberturvallisuuskeskuksen suosituksia SIEM-prosessin kehittämiseksi. Kaikki suositukset eivät varmasti sovi jokaiselle ja listasta puuttuu toisille tärkeitä kohtia mutta näiden yleisten ohjeiden perusteella voi SIEM-prosessia lähteä hahmottelemaan:

1. Määrittele organisaation lokipolitiikka
2. Vie lokipolitiikka käytäntöön kaikkiin järjestelmiin ennen SIEM-järjestelmän suunnittelua
3. Arvioi ja määrittele mitä SIEM-järjestelmä ja SIEM-prosessin käyttöönotolla tavoittelet
4. Aloita kevyesti esimerkiksi yhdellä lokipalvelimella, muutamalla lokilähteellä ja komentorivipohjaisella korrelaatioiden testauksella.
5. Älä haukkaa liian suurta palaa ja yritä saada kaikkea mahdollista välittömästi SIEM-järjestelmän piiriin
6. Varaa aikaa ja erityisesti henkilöstä SIEM-järjestelmän ja prosessin kehittämiseen, äläkä odota pelkän tuotteen ratkaisevan kaikkia tietoturvaongelmia
7. Sitoudu SIEM-prosessiin

5 Vieraskynä: SIEM lokitiedon hyödyntämisessä

Kirjoittaja Petri Vesamäki työskentelee Insta DefSec oy:ssä verkkoturva-asiantuntijana SIEM-ratkaisujen määrittelyssä, suunnittelussa, käyttöönotossa ja kehityksessä.

SIEM kerää, tallentaa ja hyödyntää valvotun järjestelmän ja ympäristön tapahtumatietoja. Tehokkaaksi viritetty analysointijärjestelmä tarjoaa käyttäjälleen tietoturvaa, kustannussäästöjä ja kilpailuetua. Tulevaisuuden SIEM on entistä laajempi, automaattisempi ja sulautetumpi osa tuotantojärjestelmiä.

SIEM tulee sanoista Security Information and Event Management. SIEM-järjestelmä havainnoi yhden tai useamman tietoteknisen järjestelmän turvallisuuteen liittyviä tapahtumia ja tarjoaa työkalut havaintojen jatkokäsittelyyn sekä tietoa ympäristöstä käsittelyn tueksi.

SIEM:n tarjoamat hyödyntämistavat alkavat yksinkertaisesta raportoinnista ja lokien tutkimisesta ja jatkuvat aina monimutkaisten tapahtumaketjujen tunnistamiseen ja tilastolliseen analysointiin. SIEM-järjestelmällä on lokitiedon lisäksi usein muitakin syötteitä tehtävänsä toteuttamiseksi.

5.1 SIEM havainnoi, prosessoi ja tallentaa

SIEM-järjestelmän päätehtävät ovat ympäristön havainnointi, tiedon prosessointi ja havaintojen jatkokäsittely sekä kerätyn syötteen tallentaminen. Havainnoidessa tietoa kerätään tyypillisesti valvottavan järjestelmän tuottamasta lokitiedosta ja ympäristön verkkoliikenteestä. Näiden lisäksi käsittelyn tueksi voidaan kerätä ympäristöön liittyvää tietoa, kuten haavoittuvuustietoja. Muita rikastavia tietoja voivat olla esimerkiksi palvelinten ohjelmistoversiot tai verkko-osoitteet laitetiedoiksi muuntava taulukko.

Tiedon prosessointi ja havaintojen jatkokäsittely voidaan myös jaotella kolmeen osaan: automaattinen käsittely, manuaalinen analysointi ja reagoinnin työnkulku. Eli ensin järjestelmä tai ihminen tulkitsee havaintoja, minkä jälkeen suoritetaan erilaisia jatkotoimenpiteitä. Tavoitteena on minimoida manuaalisen analysoinnin ja käyttäjän toimia vaativien reaktioiden osuus tiedon prosessoinnissa.

SIEM on hyödyllisimmillään, kun tietoa ja havaintoja on paljon. Suuri määrä havaintoja tarvitsee riittävästi tallennuskapasiteettia. Havainnoista muodostuvan kokonaiskuvan tarkkuus edellyttää vastuuta pääsynvalvonnassa ja käsittelyn kontrolloinnissa.

5.2 Näkyvyyttä organisaation toimintaan

SIEM parantaa ongelmien havainnointi- ja reagointikykyä, lyhentää ongelmatilanteiden aiheuttamia tuotantokatkoja sekä ohjaa henkilöresurssit paremmin vikojen selvitykseen ja korjaukseen. Sopivien mittareiden avulla SIEM voi tarjota välineet organisaation muunkin toiminnan tehostamiseen. Harva SIEM:n käyttöönottanut organisaatio on vielä näin pitkällä järjestelmänsä kanssa, mutta mahdollisuudet ovat kuitenkin olemassa.

SIEM tuo samanlaista turvaa kuin vakuutus. Yksikin selvitetty tietomurto tai ajoissa löydetty haittaohjelma saattaa hyvin tuoda takaisin koko investoinnin. SIEM:n tuoman tiedon tarjoama lisänäkyvyys organisaation toimintaan alkaa ajan myötä näkyä kilpailuetuna.

5.3 Työkalut roolien mukaan

SIEM-järjestelmän työkalut valitaan suoritettavien tehtävien mukaan. Esimerkiksi valvomohenkilöstö, turvallisuusvastaava ja ylläpitäjät tarvitsevat tehtäviinsä erilaiset välineet. Tyypillisiä kriteereitä työkalujen valintaan on kolme: tutkittavan tiedon jalostusaste ja laaja-alaisuus sekä havainnoimisen nopeus.

Valvomotoiminnassa tarvitaan havaintoja koko valvottavasta ympäristöstä nopeasti ja laaja-alaisesti. Havainnointiprosessi on pitkälle automatisoitu ja vaatii vain vähän manuaalista lisäjalostusta. Tarvetta tai kapasiteettia yksityiskohtien selvittämiseen ei juuri ole.

Turvallisuudesta tai ICT:stä kokonaisuutena vastaava henkilö tarvitsee pitkälle jalostettua tietoa laaja-alaisesti, mutta havainnoimisessa ei aina ole kyse sekunneista. Asiantuntijoiden käsittelemät havainnot ja säännöllisesti seurattavat mittarit ovat siis oikeita työkaluja jos käyntikortissa lukee vaikkapa CSO tai CISO.

Ylläpitäjät ja muut asiantuntijatehtäviä suorittavat kaipaavat näkyvyyttä sekä raakaan havaintomateriaaliin että prosessoituun tietoon. Ylläpitäjille myös nopeus merkitsee. Laajuutta voidaan usein rajoittaa vain vastuualueeseen kuuluviin järjestelmiin. Joskus näkyvyyden rajoittaminen on myös välttämätöntä vaarallisten työyhdistelmien syntymisen ehkäisemiseksi.

Minkälaisia työkaluja ylläpitäjät sitten tarvitsevat oman tehtävänsä hoitamiseen? Heillä on käytettävissään kaikki järjestelmän keräämä ja prosessoima tieto ja kaikki sen tarjoamat työkalut. Jotta SIEM-järjestelmä saadaan viritettyä tehokkaaksi, tulisi käyttäjien antaa mahdollisimman paljon palautetta kokemuksistaan, tarpeistaan ja havaitsemistaan ongelmista. Automaation kehittäminen vaatii manuaalista tiedon prosessointia.

5.4 Yksi SIEM, kiitos

SIEM-järjestelmän hankintasuunnitelma riippuu järjestelmän käyttötarkoituksesta. Minkälaisia asioita sillä halutaan havaita? Mitkä ovat oman ympäristön erityispiirteet? Mitä ovat vastuut organisaation sisällä ja ketkä järjestelmää tulevat käyttämään? Kun tavoitteet ja rajoitteet ovat selvillä, päästään miettimään järjestelmän vaatimuksia.

Käytettävien havainnointimenetelmien ja tiedonkeruun määritteleminen on kaikkein teknisin kysymys. Mistä lähteistä tietoja kerätään ja miten ne siirretään SIEM-järjestelmään? Painotetaanko havainnoinnissa luotettavuutta vai mahdollisimman vähäistä vaikutusta muuhun ympäristöön? Tämän osuuden miettimiseen kannattaa käyttää teknistä osaamista ja oman järjestelmän tuntemusta heti alusta alkaen.

Määriteltäessä tiedon prosessointia SIEM-järjestelmässä, kannattaa kysyä mitä halutaan havaita ja miten poikkeamiin reagoidaan. Havaintoja kannattaa jalostaa automaattisesti mahdollisimman pitkälle. Voidaanko heti automatisoida havaintojen tietosisällön tulkintaa, vai aloitetaanko tilastollisten poikkeamien tarkastelusta? Reaktiot ja jatkotoimenpiteet on tärkeää määritellä oikealle taholle.

Tuotetarjonta on laaja ja useimmat tarjoavat hyvin matalan käyttöönottokynnyksen. SIEM kuitenkin integroituu laajalle erilaisiin järjestelmiin tai ympäristöihin, joilla on kullakin omat erityistarpeensa. Esimerkiksi staattisen ympäristön valvonta täytyy toteuttaa puhtaasti tarkkailevilla komponenteilla mitään asentamatta. Dynaamisessa ympäristössä taas täytyy kyetä automaattisesti yhdistämään lukuisia erilaisia tunnistetietoja havaintoihin, jotta manuaalisessa analyysissa voidaan keskittyä tapahtuneen selvittämiseen osapuolten tunnistamisen sijaan.

5.5 Automaattisemmin ohjattu tulevaisuus

Spekuloidaan lopuksi hieman SIEM-järjestelmien kehitysnäkymiä tulevaisuudessa. Perusajatus tuskin muuttuu, mutta kenties SIEM-kokonaisuuteen sulautuu muita vastaavia järjestelmiä.

Valvottavien järjestelmien kirjo on jo melkoinen. Toistaiseksi SIEM integroituu lähinnä ICT-, verkko- ja joihinkin teollisuusautomaatiojärjestelmiin. Lähitulevaisuudessa SIEM havainnoi laajemmin myös tietojärjestelmiä suojaavia ja tukevia järjestelmiä, kuten kulunvalvontaa. Tilatietoisuus lisääntyy ja

tapahtumien käsittelyn tueksi kerättävät syötteet laajenevat entisestään. Verkonvalvonta, suorituskyvynvalvonta ja kulunvalvonta liittyvät tulevaisuudessa suoraviivaisemmin analyysin automatisointiin.

Laajeneeko SIEM ennen pitkää järjestelmien valvonnasta koko organisaation turvallisuuskuvan valvontaan? Työntekijöiden raportoimat turvallisuuspoikkeamat ja turvaryhmän linjaukset eivät liene helpoimpia tietolähteitä integroitavaksi, mutta eivät mahdottomiakaan. Kaikki tässä esitetyt spekulaatiot onnistuvat teknisesti jo nykyisillä SIEM-tuotteilla.

Toistaiseksi niiden toteuttaminen käytännössä on kuitenkin varsin työlästä. Entä tulisiko SIEM-järjestelmästä joskus todella itseoppiva ja omatoiminen? Tuskin. Tekniset edellytykset ovat tällekin olemassa, mutta oikeustoimikelpoisen tahon pitäminen havainnon ja reaktion välisessä päätöksenteossa ei varmaankaan poistu kovin äkkiä.

Yhteystiedot
PL 313
Itämerenkatu 3A
00181 Helsinki
puh: 0295 390 100
fax: 0295 390 270
www.viestintävirasto.fi