SeAMK
SEINÄJOEN AMMATTIKORKEAKOULU
SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Ville Santala

Kuinka vähentää SOC-tiimin manuaalista työtä automaatiolla: Microsoft Sentinel ja Logic Apps

Opinnäytetyö
Kevät 2025
Insinööri (AMK), Tietotekniikka

SEINÄJOEN AMMATTIKORKEAKOULU

Opinnäytetyön tiivistelmä

Tutkinto-ohjelma: Insinööri (AMK), Tietotekniikka

Tekijä: Ville Santala

Työn nimi: Kuinka vähentää SOC-tiimin manuaalista työtä automaatiolla: Microsoft Sentinel ja Logic Apps

Ohjaaja: Matti Panula

Vuosi: 2025 Sivumäärä: 54

Kyberuhat kehittyvät jatkuvasti, ja hyökkäysten määrä sekä monimutkaisuus kasvavat. Tämä luo yhä suuremman tarpeen hyödyntää automaatiota organisaatioiden kyberturvallisuudessa. Microsoft Sentinelin analytiikkasääntöjen tuottamien hälytysten manuaalinen käsittely kuormittaa kyberturvallisuusvalvomoiden (SOC) työntekijöitä ja hidastaa uhkien ratkaisemista, mikä voi altistaa organisaation entistä suuremmille riskeille.

Tämän opinnäytetyön tavoitteena oli kehittää Logic App -automaatiotyönkulku, joka tehostaa Microsoft Sentinelin hälytysten hallintaa. Ratkaisun avulla SOC-tiimi saa hälytykset suoraan Microsoft Teamsiin mukautuvina kortteina (Adaptive Cards), mikä nopeuttaa reagointia ja mahdollistaa suorien vastatoimenpiteiden toteuttamisen suoraan Microsoft Teams -kanavalta.

Työn tuloksena yritykselle toteutettiin Logic App -automaatio, joka parantaa Microsoft Sentinel -hälytysten hallintaa, nopeuttaa niiden käsittelyä ja tukee proaktiivista seurantaa. Automatisoitu työnkulku vähensi SOC-tiimin manuaalista työtä reitittämällä hälytykset Microsoft Teamsiin, jolloin niihin voitiin reagoida viipymättä. Tämä lisäsi SOC-tiimin reagointikykyä ja minimoi havaitsemisen ja korjaamisen välisen ajan.

[1] Asiasanat: tietoturva, kyberturvallisuus, automaatio

SEINÄJOKI UNIVERSITY OF APPLIED SCIENCES

Thesis abstract

Degree programme: Bachelor of Engineering, Information Technology

Author: Ville Santala

Title of thesis: How to reduce manual work in your SOC team with automation: Microsoft Sentinel and Logic Apps

Supervisor: Matti Panula

Year: 2025 Number of pages: 54

Cyber threats are constantly evolving, and both the number and complexity of attacks are increasing. This creates a growing need to leverage automation in organizational cybersecurity. The manual handling of the alerts generated by Microsoft Sentinel analytics rules burdens Security Operations Center (SOC) employees and slows down threat resolution.

The objective of the thesis was to develop a Logic App automation workflow to enhance the management of Microsoft Sentinel alerts. The solution was aimed to enable the SOC team to receive alerts directly in Microsoft Teams as Adaptive Cards, which would accelerate response times and allow direct countermeasures to be executed from the Microsoft Teams channel.

As the result of the thesis, a Logic App automation was implemented for the company, improving Microsoft Sentinel alert management, speeding up their resolution, and supporting proactive monitoring. The automated workflow reduced manual work for SOC team by routing alerts efficiently to Microsoft Teams, where they could be acted upon without delay. This enhanced the responsiveness of the SOC team and minimized the time between detection and remediation.

[1] Keywords: information security, cybersecurity, automation

SISÄLTÖ

Kuva-, kuvio- ja taulukkoluettelo

Käytetyt termit ja lyhenteet

Analytics rules Analytics rules, toisin sanoen analytiikat- tai analytiikkasäännöt luovat Microsoft Sentinel -hälytyksiä, kun he löytävät etsimänsä (Microsoft, 2024c). Hälytykset sisältävät tietoja havaituista tapahtumista, kuten mukana olevista entiteeteistä (käyttäjistä, laitteista, osoitteista ja muista kohteista). Hälytykset kootaan yhteen kyselyiden avulla ja korreloidaan tapahtumiksi, joita voidaan tutkia Microsoft Sentinelistä. Analytiikkasääntöjen avulla saadaan selville alustavasti uhan laajuus ja näin myös tarvittavat vastatoimenpiteet.

API Ohjelmointirajapinta eli API (Application Programming Interface) on määritelmä, jonka mukaan eri ohjelmat voivat tehdä pyyntöjä sekä vaihtaa tietoja eli toisin sanoen keskustella keskenään (IBM, 2024a). Rajapintojen avulla käyttäjälle annetaan mahdollisuus integroida erilasisia tietoja palveluita ja ominaisuuksia muista sovelluksista ja palveluista, sen sijaan että niitä lähdettäisiin kehittämään itse tyhjästä.

Entra ID Entinen Azure Active Directory (Azure AD), nykyinen Microsoft Entra ID, on pilvipohjainen identiteetin- ja pääsynhallintapalvelu (IAM), jonka avulla työntekijät voivat käyttää ulkoisia resursseja, kuten Microsoft 365:tä, Azure-portaalia ja muita SaaS (Software as a Service) -sovelluksia (Microsoft, 2025l). Entra ID tarjoaa laajan valikoiman todennusmenetelmiä, kuten monivaiheinen tunnistautuminen (MFA) sekä salasanattomia metodeja, kuten FIDO2-avaimet. Entra ID tarjoaa myös laajan valikoiman suojausominaisuuksia, kuten ehdollisen pääsyn käytännöt, (Conditional access) riskiperusteisen todennuksen ja identiteetin suojauksen (Identity protection).

Managed Identity Managed Identity eli hallinnoitu identiteetti on Azuren automaattisesti luoma identiteetti, joka mahdollistaa turvallisen ja helpon

autentikoinnin esimerkiksi Logic App -automaatiossa (Microsoft, 2025j). Hallinnoidulle identiteetille määritetään tarvittavat käyttöoikeudet, jotta sitä voidaan hyödyntää Logic App -työnkulun toiminnoissa (actions).

Microsoft Azure Microsoft Azure on Microsoftin kehittämä pilvipalvelualusta, jonka kautta yksityishenkilöt, yritykset ja julkishallinto voivat hallita, käyttää ja kehittää sovelluksia ja palveluita globaalin infrastruktuurin avulla (Microsoft, i.a.-c). Azure tarjoaa monipuolisia pilvipalvelumalleja, kuten ohjelmisto palveluna (SaaS), alusta palveluna (PaaS) ja infrastruktuuri palveluna (IaaS). Alusta tukee laajasti eri ohjelmointikieliä, työkaluja ja kehyksiä, mukaan lukien sekä Microsoftin omat että kolmansien osapuolien ratkaisut.

SIEM SIEM eli (Security Information and Event Management) on järjestelmä, joka keskittyy tietoturvatietojen ja -tapahtumien hallintaan (Palo Alto Networks. i.a.). SIEM koostuu palveluista ja työkaluista, joiden tarkoituksena on auttaa SOC (Security Operations Center) -tietoturvavalvomoita ja -toimintoja keräämään, analysoimaan ja hallitsemaan tietoturvatapahtumia. SIEM-järjestelmien keskeisiin toimintoihin kuuluu tietojen kerääminen eri lähteistä, tapahtumien yhdistäminen ja korrelaatio sekä hälytysten luominen silloin, kun yksittäinen tapahtuma tai sarja tapahtumia täyttää ennalta määritellyn SIEM-säännön.

SOAR SOAR eli (Security Orchestration, Automation and Response) tarkoittaa joukkoa palveluja ja työkaluja, jotka automatisoivat kyberhyökkäysten estämisen ja niiden käsittelyn (Palo Alto Networks, i.a.). SOAR-teknologia auttaa käytännössä automatisoimaan tehtäviä ihmisten ja työkalujen välillä yhdeltä alustalta. Tämän avulla organisaatiot voivat reagoida nopeasti kyberturvallisuusuhkiin ja hyökkäyksiin sekä tarkkailla ja ehkäistä tulevia tapauksia.

1 JOHDANTO

Nykyajan kyberturvallisuusympäristössä organisaatioiden on kyettävä reagoimaan nopeasti ja tehokkaasti erilaisiin tietoturvauhkiin. Kyberturvallisuusvalvomon (SOC) rooli on keskeinen tässä prosessissa, sillä sen vastuulla on hälytysten valvonta, analysointi ja vastatoimenpiteiden toteuttaminen (IBM, 2024b). SOC on yrityksen tietoturvayksikkö tai toisin sanoen tietoturvavalvomo, jonka pääasiallinen tehtävä on havaita, tutkia, ennakoida ja reagoida mahdollisiin tietoturvapoikkeamiin. Perinteisesti SOC-tiimin työntekijät joutuvat käsittelemään suuren määrän hälytyksiä manuaalisesti, mikä voi johtaa viiveisiin sekä resurssien kuormittumiseen. Tämän vuoksi automaation hyödyntäminen SOC-toiminnoissa on noussut yhä tärkeämmäksi osaksi organisaatioiden kyberturvallisuusstrategiaa.

Tässä opinnäytetyössä käsitellään Azure Logic App -automaation toteutusta SOC-tiimin tueksi. Microsoft Azure Logic Apps -ratkaisun avulla voidaan rakentaa automatisoituja työnkulkuja, jotka tehostavat Microsoft Sentinel -hälytyksiin reagoimista ja nopeuttavat vastatoimenpiteiden suorittamista. Automaatioiden avulla voidaan myös analysoida hälytyksiä ja suorittaa määriteltyjä toimenpiteitä ilman, että SOC-analyytikoiden tarvitsee puuttua jokaiseen hälytykseen manuaalisesti. Tämä voi vähentää merkittävästi SOC-tiimin työkuormaa ja parantaa organisaation kyberturvallisuuden reagointikykyä.

1.1 Toimeksiantaja

Työn toimeksiantajana toimi Databros Services Oy. Databros Services Oy on vuonna 2006 perustettu osakeyhtiö, jonka kotipaikka on Seinäjoki (Asiakastieto, i.a.). Yrityksen pääasiallinen toimiala on IT-ylläpito ja konsultointipalvelut.

Kesäkuussa 2024 Tietokeskus Finland Oy osti koko Databros Services Oy:n osakekannan, minkä myötä Databros Services Oy:stä tuli osa Tietokeskus-konsernia (Tietokeskus, i.a.). Tietokeskus Finland Oy on vuonna 1955 perustettu osakeyhtiö, jonka kotipaikka on Turku. Yhtiön pääasiallinen toimiala on IT-konsultointi ja IT-palvelut, ja sen toimitusjohtajana toimii Janne Lipiäinen.

1.2 Lähtötilanne

Toteutus on tehty entisen Databros Services Oy:n ympäristössä. Yrityksellä on käytössä paljon käytännöllisiä Microsoft Sentinel -analytiikkasääntöjä eri kategorioihin, tekniikoihin ja tapauksiin liittyen. Yrityksen määrittämät analytiikat tuottavat hälytyksiä Microsoft Sentinel -portaaliin, niiden havaitessa erilaisia uhkia.

Logic App -automaatiota on rakennettu myös Microsoft Sentinel -hälytysten ympärille. Yrityksen aiemman ratkaisun pohjalta Microsoft Sentinel -hälytyksistä tulee ilmoitus Microsoft Teams -kanavalle, joka sisältää tiedon asiakkaasta ja hälytyksestä sekä suoran linkin Microsoft Sentinel -hälytykseen. Analytiikan tuottamien hälytysten läpikäymiseen käytetään suurimmaksi osaksi manuaalista lähestymistapaa, eli hälytykset käydään yksitellen erikseen läpi Microsoft Sentinel -portaalissa.

1.3 Työn tavoitteet ja haettu hyöty

Työn tarkoituksena on kehittää ja testata Microsoft Sentinel -hälytyssääntöjen (toisin sanoen analytiikkasääntöjen) ympärille Logic App -automaatiota, joka puolestaan vähentää hälytysten manuaalista käsittelyä sekä nopeuttaa niiden huomaamista ja ratkaisemista.

Työn tavoiteltu tulos on luoda Azure Logic App -automaatioratkaisua hyödyntävä toteutus, joka lähettää kriittiset Microsoft Sentinel -hälytykset Microsoft Teams -palveluun mukautuvan kortin (Adaptive Card) muodossa Käytännössä tämä tarkoittaa sitä, että hälytyksen saapuessa Microsoft Sentineliin Logic App -työnkulku aktivoituu siihen määritetyn automaatiosäännön avulla ja tämän myötä Microsoft Sentinel -hälytys ajetaan välittömästi Logic App -automaation läpi sen luomisen jälkeen sekä ohjataan Microsoft Teamsiin SOC-tiimin tutkittavaksi. Logic App -työnkulussa määritetään mukautuva kortti, joka käyttää JSON-pohjaista dataa hälytyskortin rakenteeseen.

Päätavoitteena on keskittyä kriittisiin, eli vakavuudeltaan korkeimman tason hälytyksiin, jotka ohjataan Logic App -työnkulun kautta Microsoft Teamsin SOC-kanavalle tutkittavaksi. Logic App -automaation avulla voidaan nopeuttaa reagoinnin vasteaikaa kriittisiin hälytyksiin, sillä etenkin kriittiset hälytykset on hyvä ottaa työn alle mahdollisimman pian niiden syntymisen jälkeen.

Yrityksen toiveena on, että korttiin toteutetaan erilaisia painikkeita, joilla voidaan tehdä suoria vastatoimenpiteitä tarvittaessa, kuten estää käyttäjän kirjautuminen, uusia käyttäjän aktiiviset istunnot sekä nollata käyttäjän salasana.

2 MICROSOFT SENTINEL JA MUUT RATKAISUT

2.1 Microsoft Sentinel -toiminnallisuus ja -käyttö

Microsoft Sentinel, on pilvipohjainen tietoturvatietojen ja tapahtumien hallintapaneeli (SIEM) sekä suojauksen orkestrointi, automaatio ja reagointiratkaisu (SOAR) (Microsoft, 2024d). Microsoft Sentinel mahdollistaa hyökkäysten ja poikkeamien havaitsemisen, tutkimisen, niihin reagoinnin sekä uhkien ennakoivan havaitsemisen ja etsinnän. Näiden toimintojen avulla organisaatiot pystyvät havaitsemaan ja vähentämään uhkia nopeammin. Microsoft Sentinelin päätavoitteena on tarjota organisaatioille kokonaisvaltaiset turvallisuustoimet organisaatiolle tarjoamalla tiedonkeruu-, havaitsemis-, reagointi- ja tutkintavalmiuksia.

Microsoft Sentinel tarjoaa kattavan ja kustannustehokkaan pilvipohjaisen (SIEM) sekä sisäänrakennetun orkestroinnin (SOAR), joka antaa mahdollisuuden automatisoida erilaisia tehtäviä (Microsoft, 2024d). Microsoft Sentinel on erityisen hyödyllinen organisaatioille, jotka hyödyntävät jo ennestään Microsoftin tuotteita, sillä Microsoft Sentinel integroituu saumattomasti Azure-palveluihin, Defenderiin ja muihin Microsoftin tietoturvapalveluihin.

Microsoft Sentinel on yksi markkinoiden johtavista pilvipohjaisista (SIEM) ja (SOAR) ratkaisuista sen skaalautuvuuden ja helppokäyttöisyyden vuoksi, mutta Microsoft Sentinelin rinnalla on myös useita muita (SIEM) vaihtoehtoja, kuten Splunk ja IBM QRadar (Microsoft, 2024g).

2.2 Splunk Enterprise Security

Splunk Enterprise Security (ES) on joustava ja analytiikkavetoinen SIEM-ratkaisu, joka tunnetaan kyvystään käsitellä suuria datamääriä ja tuottaa syväluotaavaa tietoturva-analytiikkaa (Splunk, i.a.-a). Splunk ES sisältää valmiita korrelaatiosääntöjä ja tukee riskipohjaista hälyttämistä, mikä vähentää turhia hälytyksiä. Alusta on erittäin laajennettavissa, sillä Splunkbase-sovelluskaupasta löytyy tuhansia lisäosia ja integraatioita eri teknologioille (Splunk, i.a.-b). Splunkin käyttöliittymä tarjoaa paljon räätälöintimahdollisuuksia, mutta sen käyttö vaatii SPL-hakukielen oppimista, mikä voi aiheuttaa jyrkän oppimiskäyrän

alkuun. Hinnoittelussa Splunk tunnetaan korkeista kustannuksistaan, sillä lisensointi perustuu indeksoitavan datan määrään (Robb, 2018).

2.3 IBM QRadar

IBM QRadar on IBM:n kehittämä tietoturvatietojen ja tapahtumien hallintajärjestelmä ja se auttaa organisaatioita havaitsemaan ja vastaamaan tietoturvauhkiin koko hyökkäysketjun ajan (IBM, i.a.-a). IBM QRadar on pitkään markkinoilla ollut SIEM-ratkaisu, joka kokoaa ja korreloi loki- ja verkkoliikennetietoja, tarjoten SOC-tiimin analyytikoille keskitetyn näkyvyyden uhkiin. QRadar hyödyntää tekoälyä, valmiita sääntöjä ja käyttäytymisanalytiikkaa tehokkaaseen uhkien priorisointiin ja hallintaan (Gruner, 2024). Järjestelmä voidaan ottaa käyttöön paikallisesti tai pilvipalveluna, ja se skaalautuu lisäämällä käsittelykapasiteettia tarpeen mukaan (IBM, i.a.-b). QRadar tunnetaan erityisesti hyvästä integraatiotuestaan sekä syvällisistä hallintaominaisuuksistaan, mutta se vaatii enemmän konfigurointia ja ylläpitoa verrattuna pilvipohjaisiin vaihtoehtoihin (Pejman, 2022).

2.4 Microsoft Sentinel vs. IBM QRadar ja Splunk ES

Microsoft Sentinel on pilvipohjainen SIEM-ratkaisu, joka tarjoaa helpon käyttöönoton ilman omia palvelimia (Microsoft, i.a.-a). Microsoft Sentinel hyödyntää Azuren skaalautuvuutta ja tekoälyä automaattiseen uhkien tunnistamiseen ja hälytysmelun vähentämiseen (Microsoft, 2024a). Integraatio Microsoftin ekosysteemiin on erinomainen, erityisesti Microsoft 365 -palveluihin ja Azureen (Microsoft, i.a.-a). Kustannukset perustuvat käytettyyn datamäärään. Tiettyjen Microsoftin omien pilvipalveluiden, kuten Azure-aktiviteettilokien, Microsoft 365:n audit-lokien (Exchange, SharePoint, Teams) ja Azure Active Directoryn kirjautumis- ja audit-lokien ingestointi on Sentinelissä maksutonta (Microsoft, 2024h).

Splunk ES skaalautuu hyvin suuriin ympäristöihin ja tarjoaa laajimmat integraatiomahdollisuudet, mutta sen hinta on usein korkea ja käyttöönotto voi olla työlästä (Robb, 2018). IBM QRadar tarjoaa puolestaan joustavuutta käyttöönotossa (paikallinen/pilvi), mutta se vaatii enemmän hallintaa ja osaamista (Gruner, 2024). Sentinel erottuu edukseen helppoudellaan, erityisesti Microsoft-painotteisissa ympäristöissä, kun taas Splunk ja QRadar sopivat paremmin monimutkaisiin, monitoimittajaympäristöihin.

3 TIETOTURVAVALVOMO SOC

3.1 Mikä on SOC?

SOC (Security Operations Center) on yrityksen tietoturvayksikkö tai toisin sanoen tietoturvavalvomo, jonka pääasiallinen tehtävä on havaita, tutkia, ennakoida ja reagoida mahdollisiin tietoturvapoikkeamiin (IBM, 2024b). Kyberturvallisuusvalvomon (SOC) päätehtävänä on parantaa yrityksen kyberturvallisuutta, seurata, havaita, etsiä, ennakoida sekä estää tietoturvaan liittyviä uhkia (Microsoft, i.a.-f). SOC on joko organisaation sisäinen tai ulkoistettu tietoturva-ammattilaisten tiimi, joka valvoo organisaation koko IT-infrastruktuuria yleensä ympärivuorokautisesti. SOC-tietoturvavalvomon ympärillä toimii analyytikoita, jotka reagoivat SOC-hälytyksiin (IBM, 2024b).

3.2 SOC-tehtävät ja merkitys organisaatiossa

Vahva SOC on niin sanottu tukipylväs, joka auttaa yrityksiä pysymään aallonharjalla kehittyvien kyberuhkien keskellä niiden muuttuessa ja vaikeutuessa jatkuvasti (Microsoft, i.a.-f). Kyberuhat kehittyvät sekä muuttuvat jatkuvasti yhä haastavimmiksi huomata ja jäljittää, etenkin kyberrikollisille tekoälyn tuomien mahdollisuuksien myötä. SOC-tiimillä on suuri merkitys yrityksessä, sillä tätä kautta valvotaan reaaliaikaisesti organisaation käyttäjätietoja, päätepisteitä, palvelimia, tietokantoja, verkkosovelluksia, sivustoja ja muita järjestelmiä mahdollisten hyökkäysten varalta (Microsoft, i.a.-f).

SOC-tiimit (toisin sanoen SOC-analyytikot) käyttävät SIEM- ja SOAR-työkaluja, kuten esimerkiksi Microsoft Sentineliä tietoturvatapahtumien hallintaan (IBM, 2024b). SOC-tiimit toteuttavat toimenpiteitä kyberhyökkäyksiä vastaan tarvittaessa, ja täten suurin osa SOC-tiimeistä toimiikin kellon ympäri seitsemänä päivänä viikossa. SOC käyttää toiminnassaan myös data-analytiikkaa, lokeja sekä ulkoisia syötteitä kerätäkseen tarvittavia tietoja hyökkääjän toiminnasta, motiiveista ja infrastruktuurista. SOC-tiimit keräävät tietoa, miksi ja miten tietyt kyberrikollisten ryhmät sekä trendit toimivat ja näiden tietojen avulla puolestaan voidaan vahvistaa yrityksen tietoturvaa entisestään (IBM, 2024b). SOC-tiimin vastuulle kuuluu yleensä myös yrityksen tilan palauttaminen entiselleen hyökkäysten jälkeen.

3.3 SOC-automaatio ja edut

SOC-automaatioilla tarkoitetaan käytännössä siis automatisointia organisaation SOC-ympäristössä ja ne hyödyntävät teknologioita kuten SOAR ja SIEM, jotta tietoturvapoikkeamien havaitseminen, analysointi, ja reagointi voitaisiin toteuttaa nopeammin ja tehokkaammin (Cross, 2024). Kyseinen automatisointiprosessi voidaan toteuttaa osalle tai kaikille SOC-toimintojen osa-alueille sekä oikeanlaisista automaatioista on suuri hyöty organisaatiolle, sillä automatisoinnilla voidaan korvata päivittäisiä manuaalisia suojaus- ja valvomistoimenpiteitä sekä lisätä nopeutta ja tehokkuutta. Automaatioita voidaan käyttää esimerkiksi saapuneiden hälytysten tietojen rikastamiseen sekä automaattisten vastatoimenpiteiden suorittamiseen.

Automaatioiden tarve kasvaa yhä enemmän tulevaisuudessa, sillä se nopeuttaa saapuneiden hälytysten ratkaisemista, tarvittavien lisätietojen noutoa, vähentää toistuvia manuaalisia prosesseja sekä helpottaa välittömien toimenpiteiden suorittamista ja hälytysten rikastamista (Cross, 2024). Automaatio on hyvä ratkaisu etenkin yritykselle, jossa ei ole ympärivuorokautista SOC-tiimiä, sillä suurin osa toimenpiteistä voidaan toteuttaa suoraan oikeanlaisen automaation avulla. Automatisoiduilla prosesseilla on mahdollista vaikuttaa myös organisaation resurssipulaan, eli osa toiminnoista voidaan automatisoida ja näin vähentää SOC-tiimin taakkaa sekä käsiteltävien hälytysten määrää.

SOC-automaatio on kokonaisuudessaan keskeinen osa nykyaikaista tietoturvaa, SOC-automaation avulla organisaatiot voivat reagoida uhkiin nopeammin, vähentää manuaalisia prosesseja ja parantaa yleisesti uhkien havainnointia (Cross, 2024). Automaatioilla voidaan myös yhdistää eri järjestelmien ja palveluiden tiedot ja analysoida niitä keskistetysti, mikä mahdollistaa puolestaan paremman tilannekuvan uhkien leviämisestä ja kriittisyydestä.

3.4 SOC-automaatioiden haasteet ja rajoitukset

Vaikka yleisellä tasolla SOC-automaatiot tarjoavat loistavia etuja yritykselle, niiden käyttöönottoon, konfigurointiin ja hallintaan liittyy myös haasteita (Cross, 2024). Yksi suurimmista haasteista on väärät positiiviset tulokset (false positives), joissa SOC-järjestelmät voivat luoda vääriä hälytyksiä ja näin myös automaatiot voivat tehdä vääriä toimenpiteitä.

Automaatioiden konfigurointi voi tuottaa myös haasteita, sillä väärin määritetty automaatio voi esimerkiksi sulkea työntekijän tilin väärin perustein sekä toteuttaa virheelliset korjaustoimenpiteet. Kokonaisuudessaan SOC-tiimien on siis ymmärrettävä, miten automaatio ja analytiikat toimivat, jotta voidaan välttää väärät toimenpiteet ja konfiguroida työnkulku oikein.

Automaatioiden konfigurointiin liittyykin uusien ja olemassa olevien automaatioiden jatkuva testaus, muokkaus sekä manuaalinen tarkistus ennen tuotantoon lisäämistä (Cross, 2024). Automaatioissa on myös rajoituksia, eli osa tapauksista vaatii edelleen ihmisen päätöksentekoa tuekseen, jotta oikeita vastatoimenpiteitä voidaan suorittaa erilaisissa tilanteissa. Yleisesti automaatioiden toteutus vaatii huolellista suunnittelua ja pohdintaa, mitä prosesseja on järkevä automatisoida ja mitä ei.

4 AZURE LOGIC APPS AUTOMAATIORATKAISUNA SENTINELISSÄ

4.1 Azure Logic Apps -teknologia ja sen toiminta

Azure Logic Apps on Microsoftin tarjoama pilvipohjainen palvelu, jonka avulla voidaan toteuttaa erilaisia integraatioita ja työnkulkuja ilman laajaa ohjelmointiosaamista (Microsoft, 2025c). Kyseinen palvelu edustaa niin sanottua low-code/no-code-teknologiaa, eli sen käyttö ei edellytä käyttäjältä perinteistä ohjelmointia tai sen opettelemista. Logic Apps mahdollistaa automaatiot ja järjestelmien väliset tiedonsiirrot hyödyntämällä valmiita liittimiä sekä kolmansien osapuolien ohjelmistojen välisiä (API) rajapintoja (Application Programming Interface).

Azure Logic Apps on niin sanottu iPaaS (Integration Platform as a Service), eli käytännössä se toimii yhdistämällä erilaisia järjestelmiä, sovelluksia ja tietolähteitä mahdollistaakseen saumattoman viestinnän ja automatisoinnin (Microsoft, 2025f). Logic Apps tarjoaa satoja valmiita liittimiä (Connectors), jolla saadaan yhdistettyä sekä integroitua erilaisia työnkulkuja eri palveluihin, järjestelmiin, sovelluksiin ja tietoihin.

Logic Apps -työnkulkujen toteuttamiseen Microsoft tarjoaa käyttäjälle visuaalisen suunnittelualustan (Logic App Designer), jonka avulla työnkulut suunnitellaan ja toteutetaan (Microsoft, 2025c). Tämän suunnittelualustan avulla voidaan rakentaa monimutkaisiakin automaatiotyönkulkuja ilman, että käyttäjän tarvitsee itse kirjoittaa laajoja koodirivejä. Logic App -työnkulut koostuvat laukaisintoiminnoista (trigger) eli toiminnoista, jotka käynnistävät työnkulun, sekä erilaisista toiminnoista (actions), jotka määrittävät, mitä Logic App automaation käynnistyksen jälkeen tehdään (Microsoft, 2025g). Toiminnot voivat sisältää esimerkiksi tietokantakyselyitä, ilmoitusten lähettämistä tai hälytykseen liitettyjen käyttäjien listaamista.

4.2 Automaatiosääntöjen määrittäminen Microsoft Sentinelissä

Automaatiosäännöt ovat keskeinen osa Azure Logic Appsin hallintaa Microsoft Sentinel -ympäristössä (Microsoft, 2024b). Automaatiosääntöjen avulla voidaan keskitetysti hallita ja ohjata automaatioiden suorittamista, mikä parantaa hälytysten käsittelyprosessia.

Automaatiosäännöissä määritetään erilaisia ehtoja, joiden perusteella tarkistetaan täyttyvätkö tietyt kriteerit ennen kuin Logic App -työnkulku käynnistetään. Automaatiosäännöt mahdollistavat esimerkiksi sen, että vain sääntöön määritetyt Microsoft Sentinel -analytiikat tai määritetyn vakavuuden (Informational, Low, Medium, High) hälytykset laukaisevat tietyn Logic App -automaation.

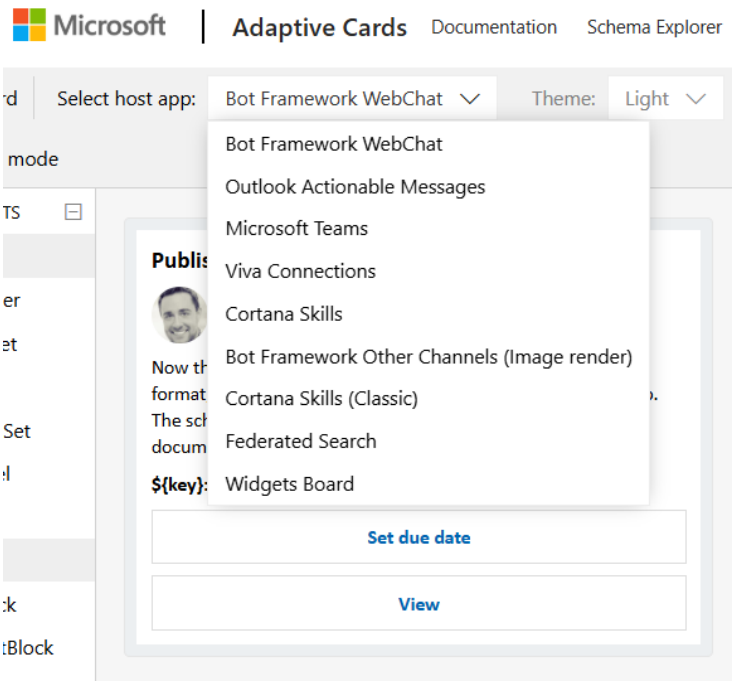
4.3 Adaptive Cards teknologia ja sen käyttömahdollisuudet

Mukautuvat kortit (Adaptive Cards) on Microsoftin kehittämä avoimen standardin viestintäteknologia, joka mahdollistaa interaktiivisten korttien luomisen ja esittämisen eri sovelluksissa ja palveluissa (Microsoft, 2021). Mukautuvat kortit, tarjoaa dynaamisen ja modulaarisen tavan esittää tietoa ja sitä voidaan hyödyntää esimerkiksi Microsoft Teams -ilmoituksissa ja -kyselyissä sekä Microsoft Outlookissa.

Mukautuvien korttien (Adaptive Cards) toiminta perustuu JSON-pohjaiseen rakenteeseen, joka mahdollistaa kortin sisällön ja toiminnallisuuden muokkaamisen dynaamisesti (Microsoft, 2023). Mukautuvien korttien käyttö on erinomainen ratkaisu Logic App -automaatioiden rinnalle Microsoft Sentinel -hälytysten hallintaan. Mukautuvia kortteja voidaan hyödyntää päätöksen, ja vastauksien toteuttamiseen esimerkiksi suoraan Microsoft Teams -kanavalta.

4.3.1 Adaptive Card Designer

Adaptive Cards Designer on selainpohjainen työkalu, jonka avulla voidaan suunnitella ja esikatsella mukautuvia kortteja (toisin sanoen Adaptive Cards) ilman koodin kirjoittamista (Microsoft, 2021). Mukautuvat kortit käyttävät JSON-pohjaista muotoilua, jota käytetään esimerkiksi interaktiivisten käyttöliittymäelementtien luomiseen eri sovelluksissa ja palveluissa, kuten Microsoft Teams-, Outlook- ja Windows-ilmoitukset.



Kuva 1. Adaptive Cards Designer -alusta.

Adaptive Cards Designerillä voidaan suunnitella ja toteuttaa kortteja visuaalisesti ilman manuaalista JSON-koodausta (Riyani, 2024). Adaptive Cards Designer mahdollistaa myös korttien esikatselun käytetyssä ympäristössä, kuten Microsoft Teams -palvelussa tai Microsoft Outlookissa. Näin saadaan varmistettua niiden oikea ulkoasu. Adaptive Card Designer -alusta generoi automaattisesti kortille JSON-muotoisen koodin, jota voidaan käyttää sekä hyödyntää eri palveluissa ja sovelluksissa.

4.3.2 Adaptive Cards -työkalun käyttö Microsoft Sentinel -hälytysten hallinnassa

Logic App -työnkulun kautta lähetettävien mukautuvien korttien avulla voidaan hallita Microsoft Sentinel -hälytyksiä suoraan Microsoft Teamsin kautta (Microsoft, 2022). SOC-tiimin jäsenet voivat esimerkiksi tehdä seuraavia toimenpiteitä korttien kautta ilman, että heidän tarvitsee avata Microsoft Sentinel -portaalia (Microsoft, 2022):

- Tarkastella Microsoft Sentinel -hälytyksen tietoja ilman, että heidän tarvitsee avata Microsoft Sentinel -portaalia.
- Suorittaa ennalta määritettyjä toimenpiteitä, kuten käyttäjän salasanan nollaus, istunnon uusiminen, tilin estäminen tai hälytyksen sulkeminen.
- Lisätä kommentteja Microsoft Sentinel -hälytyksiin, joita muut SOC-tiimin jäsenet voivat hyödyntää.

Mukautuvien korttien (Adaptive Cards), ohjelmointirajapintojen (API) ja Logic Appien yhdistelmällä voidaan nopeuttaa hälytysten käsittelyä sekä helpottaa SOC-tiimin analyytikoita tekemään päätöksiä ja toteuttaa tarvittavia vastatoimenpiteitä (Microsoft, 2022).

5 AUTOMAATION RAKENTAMINEN JA TESTAUS

5.1 Valmistelut ja vaatimukset

Logic App -automaation toteuttaminen aloitettiin keskustelemalla yrityksen tarpeista ja vaatimuksista sekä millaisia hälytyksiä olisi järkevä lähettää automaatioiden kautta Microsoft Teamsin SOC-kanavalle.

Yrityksen käytössä oli valmiina Azure-testiympäristö, joka ei ole liitettynä asiakkaisiin tai muihin resursseihin. Testiympäristöä hyödynnettiin Logic App -automaation testaamisessa ja toteutuksessa, ennen tuotantoon lisäämistä. Testiympäristössä on valmiiksi aktiivisena Microsoft Sentinel -analytiikkasääntöjä, joiden avulla voidaan suorittaa testitapauksia sekä testata Logic App -automaation toimintaa.

Automaation toiminnan testaukseen ja toteuttamiseen tarvittavat resurssit:

- Testikäyttäjä
- Microsoft Sentinel -analytiikkasäännöt
- Logic App -automaatio (Playbook)
- Tarvittavat käyttöoikeudet Logic Appin suorittamiseen
- Hallittu identiteetti (Managed Identity) Logic Appille
- Rekisteröity sovellus (App registration)
- Automaatiosääntö

Tapauksen kulku:

- Microsoft Sentinel -analytiikkasääntö luo hälytyksen Microsoft Sentineliin.

- Microsoft Sentinel -automaatiosääntö tarkistaa täyttyykö siihen määritelty ehto, ja käynnistää Logic App -automaation. Logic App -automaatio käsittelee hälytyksen tietoja, ja lähettää siitä mukautuvan kortin (Adaptive Card), Microsoft Teamsin SOC-kanavalle.

- Logic App -työnkulun kautta Microsoft Teams -kanavalle lähetetty mukautuva kortti (Adaptive Card), sisältää tiedon hälytykseen liittyvästä asiakkaasta, käyttäjästä, mikä Microsoft Sentinel -analytiikka loi hälytyksen sekä vaihtoehdot toteuttaa vastatoimenpiteitä.

- Mukautuvaan korttiin painikkeet, joilla voidaan toteuttaa vastatoimenpiteitä tarvittaessa:

    - Disable user: Estää käyttäjän kirjautumisen, kirjautuminen estetään Microsoft Entra ID:n (entinen Active Directory) kautta.

    - Reset password & revoke sessions: Nollaa käyttäjän salasanan ja uusii aktiivisena olleet istunnot. Uusi väliaikainen salasana palautetaan Microsoft Teamsin SOC-kanavalle mukautuvan kortin muodossa, josta se voidaan toimittaa asiakkaalle myöhemmin.

    - Close incident: Sulkee hälytyksen Microsoft Sentinelistä.

    - Ignore: Hylkää mukautuvan kortin Microsoft Teamsista, mutta ei tee muita toimia käyttäjätileihin tai Microsoft Sentinel -hälytykseen liittyen.

Logic App -työnkulkua testattiin testiympäristön Microsoft Sentinel -hälytysten ja testikäyttäjän avulla ennen tuotantoon lisäämistä.

5.2 Toimintojen suunnittelu

Ensimmäisenä otettiin selvää, onko olemassa valmiita ratkaisuja haluttujen vastatoimenpiteiden sekä mukautuvan kortin (Adaptive Card) toteuttamiseen. Microsoftilla oli valmiita Logic App -automaatioita (Playbook) istuntojen nollaamiseen (Revoke sessions), käyttäjän

sulkemiseen (Disable user), mutta mukautuvaan korttiin (Adaptive Card) ei löydetty suoraa ratkaisua, jossa olisi valmiina painikkeet tai rakenne, jota voitaisiin hyödyntää toimintojen aktivoimiseen Logic App -työnkulussa.

5.3 Tarvittavat käyttöoikeudet Logic Appille

Logic App -automaatiot tarvitsevat aina jonkun tasoisia käyttöoikeuksia toimiakseen varsinkin jos automaation kautta toteutetaan toimenpiteitä käyttäjätileille. Tämän automaation tavoitteena on tarjota SOC-tiimin analyytikoille mahdollisuus toteuttaa toimenpiteitä mukautuvan kortin painikkeiden avulla suoraan Microsoft Teamsista. Toimenpiteiksi toteutettiin: disable user, reset password & revoke sessions ja close incident. Toimenpiteiden suorittamiseen täytyi määrittää tarvittavat käyttöoikeudet Logic Appissa hyödynnettävälle hallitulle identiteetille (managed identity) ja rekisteröidylle sovellukselle (app registration).

Käytetyt käyttöoikeudet:

- Microsoft Sentinel Responder -rooli:
    - Tarvitaan Sentinel-hälytysten hallintaan ja reagointitoimiin (käytetään ”Update Incident” -toiminnolle).
- Password Administrator -rooli:
    - Annetaan Logic Appin hallitulle identiteetille, joka lisätään PowerShellin avulla (käytetään ”Reset password”-toiminnolle).
- Microsoft Graph API (Application-oikeudet):
    - User.ReadWrite.All – mahdollistaa käyttäjätietojen lukemisen ja muokkaamisen (käytetään ”Revoke”-toiminnolle).
    - User.EnableDisableAccount.All – mahdollistaa kirjautumisen estämisen käyttäjiltä (käytetään ”Disable”-toiminnolle).
    - SecurityIncident.ReadWrite.All – tarvitaan tietoturvahälytysten käsittelemiseen Graphin kautta.

Käyttöoikeudet voidaan määrittää esimerkiksi PowerShellin kautta managed identitylle tai erikseen rekisteröidylle sovellukselle (app registration) Microsoft Entra ID:stä. Tässä

toteutuksessa käytettiin molempia sekä hallittua identiteettiä (managed identity) että sovellusrekisteröintiä (app registration).

5.4 Microsoft Teams -hälytyskortin rakenteen suunnittelu ja toteutus

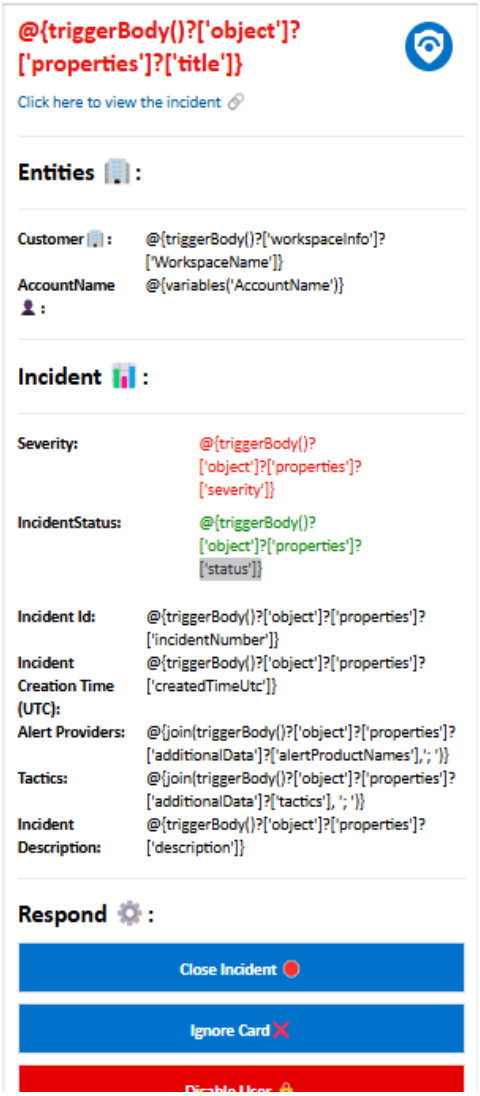
Mukautuvalle kortille, jonka tarkoituksena on lähettää Microsoft Sentinel -hälytyksestä kortti Microsoft Teamsin SOC-kanavalle, suunniteltiin rakenne, josta tulee ilmi kaikki tarvittavat tiedot hälytykseen liittyen sekä painikkeet vastatoimenpiteiden suorittamiseen. Kortin toteutukseen hyödynnettiin Microsoftin dokumentaatiosta löytyvää mukautuvien korttien suunnittelualustaa (Adaptive Cards designer), jonka kautta voi suunnitella ja toteuttaa mukautettuja kortteja suoraan Microsoft Teams -palveluun (Microsoft, 2025d).

Kortille suunniteltu rakenne:

- Tieto, mitä asiakasta Microsoft Sentinel -hälytys koskee.
- Mikä käyttäjä tai käyttäjät ovat liitettynä hälytykseen (Entities).
- Tiedot hälytykseen liitetystä Microsoft Sentinel -analytiikasta:
    - Hälytyksen otsikko (Rule Name)
    - Hälytyksen vakavuus (Severity)
    - Hälytyksen tila (Incident Status)
    - Analytiikan kuvaus (Description)
    - Taktiikka (Tactics)
- Toimenpidevaihtoehdot painikkeiden muodossa
    - Disable user
    - Reset password & revoke sessions
    - Close incident
    - Ignore
    - Revoke (väliaikaiseen testaamiseen)

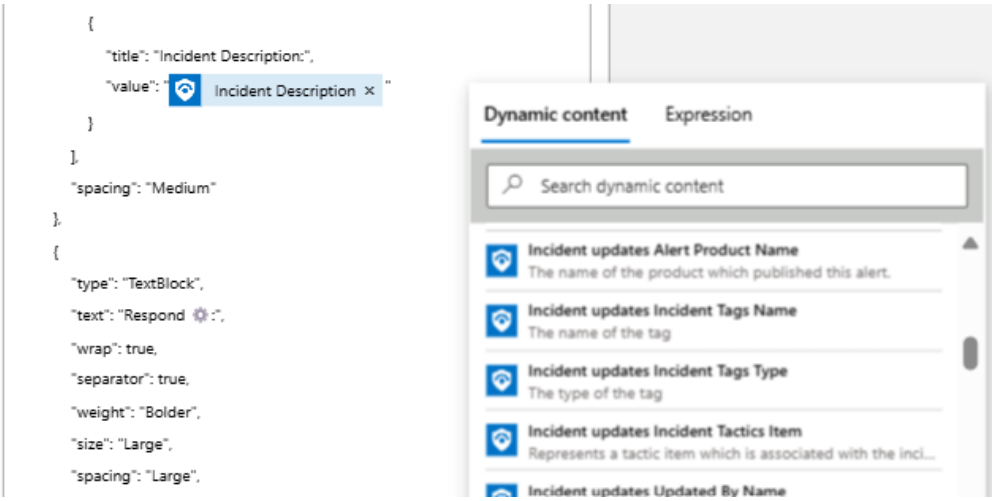
5.4.1 Mukautuvan kortin toteutus (Adaptive Card Designer)

Mukautuvassa kortissa hyödynnettiin Logic App -työnkulun tarjoamaa dynaamista sisältöä, jotta halutut tiedot saatiin näkyviin suoraan korttiin. Korttiin toteutettiin kuvan 2 mukainen rakenne, josta saadaan selville asiakas, käyttäjä tai käyttäjät, hälytyksen vakavuus, Microsoft Sentinel -analytiikkasäännön otsikko ja kuvaus sekä erilliset painikkeet toimenpiteille.



Kuva 2. Mukautuvan kortin (Adaptive Card) suunniteltu rakenne.

Mukautuvan kortin eri osioihin määritettiin suoraan kuvan 3 mukaisesti Logic App -työnkulun tarjoamaa dynaamista sisältöä, Microsoft Sentinel -laukaisintoiminnosta (trigger). Dynaamisen sisällön liittäminen mukautuvan kortin eri osioiden (value) kenttään mahdollisti haluttujen tietojen noutamisen suoraan saatavilla olevista hälytyksen tiedoista.

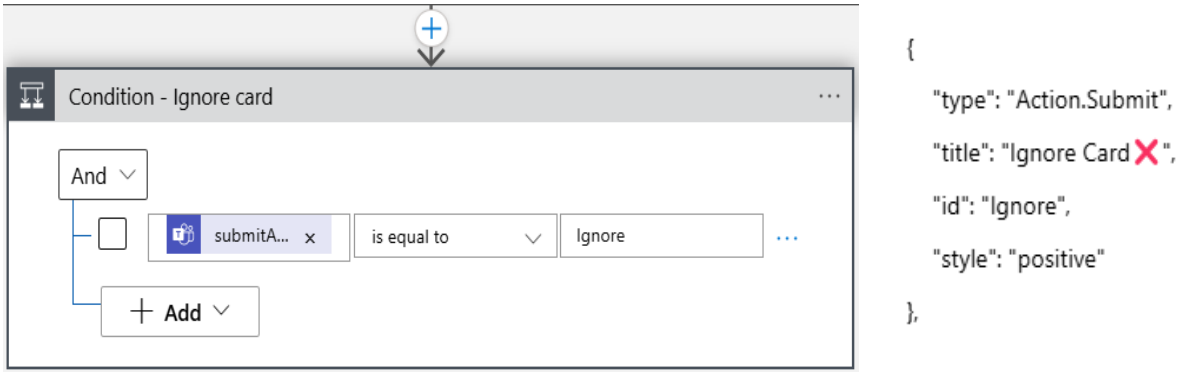


Kuva 3. Microsoft Sentinelin dynaamisen sisällön käyttö mukautuvassa kortissa.

5.5 Toimintojen suorittaminen mukautuvasta kortista

Mukautuvan kortin jokainen painike eriteltiin id-arvolla mukautuvien korttien suunnittelualustalla (Adaptive Cards Designer), jotta niitä voitiin käyttää toteuttamaan eri toimenpiteitä Logic App -työnkulussa. Logic Appin täytyy tunnistaa, mitä painiketta on painettu, jotta se voi siirtyä työnkulussa eteenpäin suorittamaan kullekkin painikkeelle erikseen määritetyt toimenpiteet.

Tähän keksittiin ratkaisuna työnkulussa ehtolausekkeen hyödyntäminen (Condition), joka puolestaan tarkistaa painetusta painikkeesta sille määritetyn yksilöidyn tunnisteen (id) ja ohjaa Logic App -työnkulun erilliseen rinnakkaiseen haaraan (Parallel branch), jossa suoritetaan kullekin painikkeelle erikseen määritetyt toimenpiteet.



Kuva 4. Ehtolauseke tarkistamaan napin painallus kortista id-arvolla.

Mukautuvan kortin rakennetta toteuttaessa määritettiin jokaiselle painikkeelle oma yksilöity tunnus (id), jolla painikkeet eroteltiin. Näin kullakin painikkeella voitiin suorittaa eri toimenpiteitä. Mukautuvan kortin painikkeet toteutettiin korttien suunnittelualustalla Adaptive Cards Designer Microsoftin virallisen dokumentaation mukaan toiminnolla Action.Submit (Microsoft, i.a.-g). Logic App -työnkulun ehtolausekkeessa (Condition) viitattiin mukautuvan kortin painikkeisiin ja tehtiin tarkistus painikkeen yksilöidyn tunnisteen (id) avulla kuvan 4 mukaisesti.

5.6 Käyttäjän kirjautumisen estäminen kortista

Mukautuvalle kortille määritettiin painike, jonka avulla käyttäjän kirjautuminen voidaan estää. Toiminnon toteutustapaa selvittäessä havaittiin, että se on mahdollista suorittaa Microsoft Graph -rajapinnan (Microsoft Graph API) kautta. Tämä mahdollisti sen, että Microsoft Graph -rajapintaa voitiin hyödyntää yhdessä Logic Appin kanssa käyttäjähallintaan liittyvien toimenpiteiden automatisoimiseksi Microsoft Entra ID:ssä.

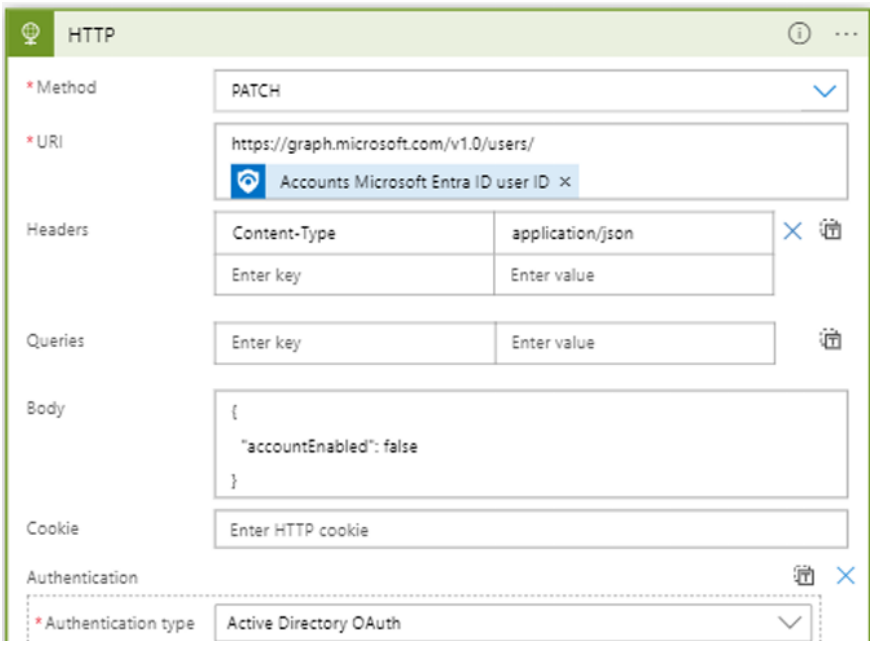
Logic App -työnkulussa Microsoft Graph -rajapintoja voitiin kutsua suoraan ilman erillistä ohjelmointia tai koodia HTTP-toiminnolla (action). Työnkulku haki hälytykseen liitetyn käyttäjän (Entity) yksilöidyn tunnisteen (user ID) ja käyttäjän kirjautumisen estäminen suoritettiin Microsoft Graph -rajapinnan kautta.

Toiminto olisi mahdollista myös automatisoida kokonaan erillisellä Logic App -automaatiolla osana tietoturvatapahtumien hallintaa, mutta yrityksen toiveena oli antaa vain mahdollisuus toteuttaa toimenpide tarvittaessa, eli sitä ei toteuteta itsenäisesti suoraan Logic App -automaation toimesta. Kirjautumisen estäminen käyttäjälle on erityisen hyödyllinen

tilanteissa, joissa havaitaan epäilyttävää käyttäjätoimintaa tai jopa tilin kaappaaminen. Käyttäjätilin päivittäminen Microsoft Graph -rajapinnan kautta on suoritettavissa käyttämällä asianmukaisia käyttöoikeuksia ja hyödyntämällä PATCH-metodia Logic App -työnkulun HTTP-toiminnossa (Microsoft, 2025b).

5.6.1 HTTP-toiminnon määrittely

Itse HTTP-toiminto määriteltiin Logic App -työnkulussa seuraavasti:



Kuva 5. HTTP-toiminto estämään käyttäjän kirjautuminen.

Microsoft Graph API mahdollistaa Microsoft Entra ID -käyttäjätilien hallinnan, mukaan lukien tässä tapauksessa käyttäjän kirjautumisen estämisen. Logic App -työnkulussa hyödynnettiin HTTP-pyyntöä Microsoftin virallisen dokumentaation mukaisesti, se lähettää PATCH-pyynnön Microsoft Graph API:n käyttäjäresurssiin (Microsoft, 2025b). Pyynnön runkoon määritettiin JSON-rakenne, jossa käyttäjätilin (accountEnabled) arvon tosi (true) sijaan asetetaan arvo epätosi (false), jolloin kirjautuminen tilille estetään tilapäisesti.

Pyynnön otsikkotietoihin (headers) määriteltiin sisällön tyypiksi JSON sekä pyynnön autentikointiin käytettiin Logic Appia varten tarvittavilla käyttöoikeuksilla määritetyn sovelluksen (app registration) tunnistetietoja (clientId & secretId).

Autentikoinnissa käytetylle rekisteröidylle sovellukselle (app registration) määritettiin User.EnableDisableAccount.All-käyttöoikeudet Microsoft dokumentaation mukaisesti (Microsoft, 2025b).

Vain tarvittavien oikeuksien määrittäminen on yksi keskeisimmistä hyvistä tietoturvakäytännöistä, käyttäjille, järjestelmille ja prosesseille annetaan vain ne oikeudet, jotka ovat välttämättömiä niiden tehtävien suorittamiseksi.

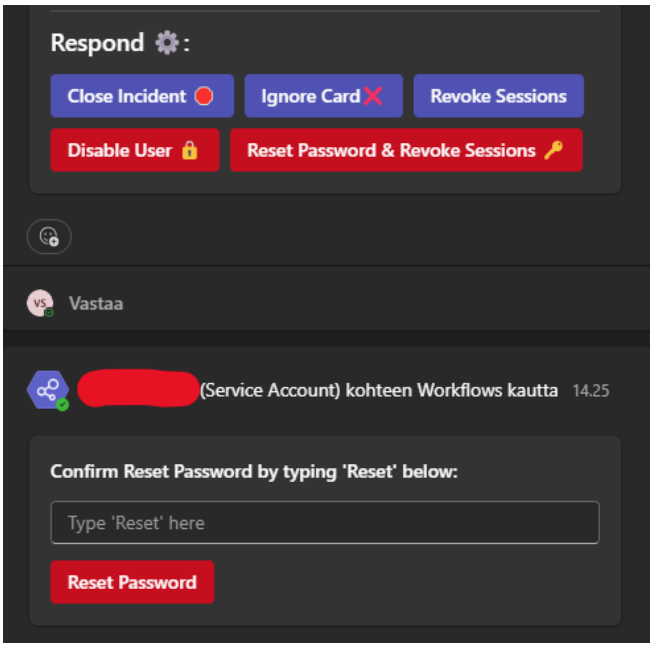
5.7 Salasanan ja istuntojen nollaus

Käyttäjän salasanan ja istuntojen uusiminen toteutettiin yhtenä toimenpiteenä, mikä on tyypillistä, sillä pelkkä salasanan vaihtaminen ei välttämättä aina riitä, jos hyökkääjällä on jo aktiivinen istunto jossakin palvelussa.

Kyseinen toiminto suorittaa kaksi toimenpidettä Graph API:n avulla ja ne toteutetaan hälytyksen tarkastelijan painaessa mukautuvasta kortista ”Reset Password & Revoke Sessions” -painiketta. Näiden molempien vaiheiden toteuttamiseen voitiin käyttää samaa lähestymistapaa kuin käyttäjätilin sulkemisessa eli Graph API -pyyntöä.

5.7.1 Lisävahvistus toiminnon suorittamisesta

Painiketta (Reset Password & Revoke Sessions) painettaessa pyydetään käyttäjältä kuvan 6 mukainen lisävahvistus ennen toiminnon suorittamista.



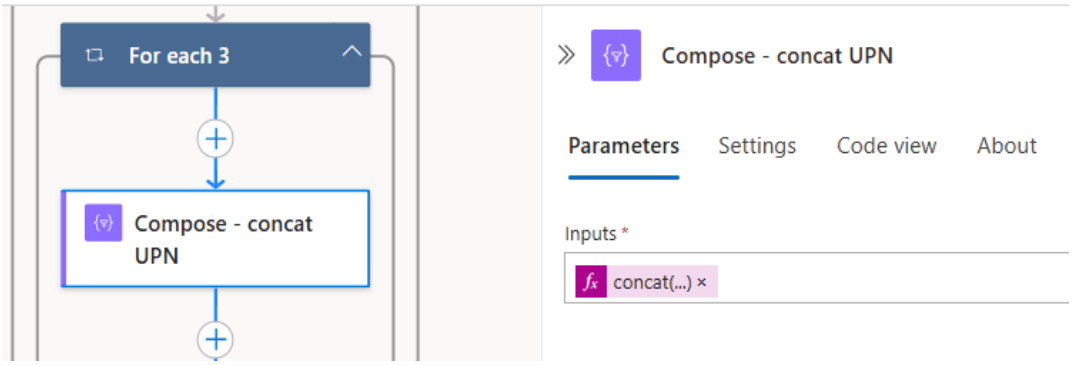
Kuva 6. Lisävahvistus toiminnon suorittamisesta.

Vahvistus vaaditaan kaikissa kriittisemmissä toimenpiteissä, kuten esimerkiksi käyttäjän salasanan nollaamisessa tai kirjautumisen estämisessä. Jokaiselle toiminnolle on erikseen määritetty ehdot (Condition), jotka tarkistavat painikkeen toiminnan ja edellyttävät tarvittaessa lisävahvistusta. Tarkistuksissa hyödynnetään painikkeen yksilöityä tunnistetta (id), joka on määritetty mukautuvalle kortille etukäteen painikkeiden (Action.Submit) alle. Lisävahvistuksissa käyttäjän tulee syöttää pyydetty teksti kuvan 6 mukaisesti, jotta toiminto vahvistetaan ja suoritetaan.

5.7.2 Toiminnon suorittaminen

Kun lisävahvistus on tarkistettu ja hyväksytty onnistuneesti Logic App -työnkulussa, toteutetaan pyydetty toiminto. Logic Appissa yhdistettiin käyttäjän nimi (AccountName) ja loppuosa (UPNSuffix) yhdeksi tunnukseksi käyttäen välissä @-merkkiä sekä hyödyntämällä Logic Appin compose -toimintoa ja sen sisällä concat-funktiota.

- concat(items('For_each_3')?['Name'], '@', items('for_each_3')?['UPNSuffix'])

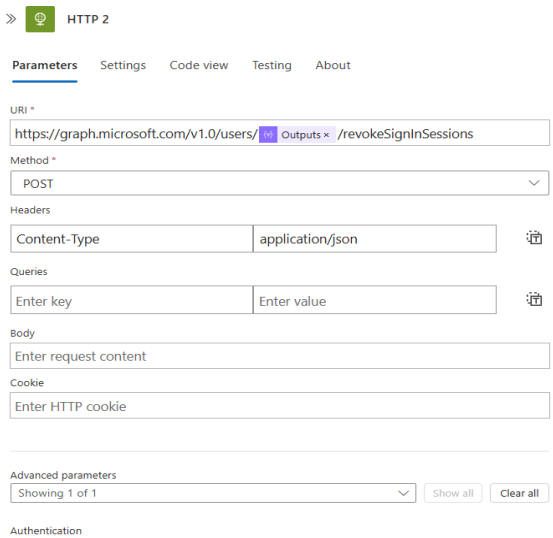


Kuva 7. Concat-funktio yhdistämään käyttäjän sähköpostiosoite.

Kyseinen funktio yhdistää tiedot yhdeksi kokonaiseksi tunnisteeksi käyttäjän tiedoista muotoon nimi.sukunimi@yritys.fi. Tätä tunnusta puolestaan hyödynnetään Graph-rajapinnan pyynnössä, joka toteuttaa itse toimenpiteen käyttäjän tilille.

5.7.3 Istuntojen nollaus

Istuntojen ja käyttäjän salasanan nollaus toteutettiin Microsoft Graph -rajapintaa hyödyntäen erillisessä Logic App -työnkulun HTTP-toiminnossa.

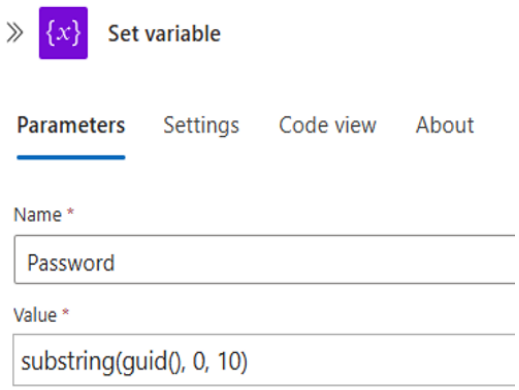


Kuva 8. Käyttäjän istuntojen uusiminen Graph-rajapintaa hyödyntäen (Revoke).

Toiminto (Revoke) mitätöi käyttäjän aktiiviset istunnot eli tämä kirjaa käyttäjän ulos kaikista laitteista ja pakottaa uudelleen kirjautumisen. Kyseinen toiminto suoritettiin työnkulussa hyödyntäen jälleen Microsoft Graph -rajapintaa. Toiminnon suorittamiseen tarvittiin oikeanlaiset käyttöoikeudet, jotta toimenpide saatiin suoritettua onnistuneesti. Microsoftin virallisen dokumentaation mukaan riittävät oikeudet olivat User.RevokeSessions.All- tai puolestaan korkeammat oikeudet User.ReadWrite.All, joita käytettiin tämän toiminnon testaamisessa (Microsoft, 2025e)

5.7.4 Salasanan nollaus

Salasanan nollausta varten lisättiin tyhjä (Intialize variable) -muuttuja, johon lisättiin käyttäjälle väliaikainen salasana kuvan 9 mukaisesti Set variable -toiminnolla. Satunnainen salasana toteutettiin Set variable -toiminnossa käyttäen aiemmin lisättyä tyhjää muuttujaa (Password).

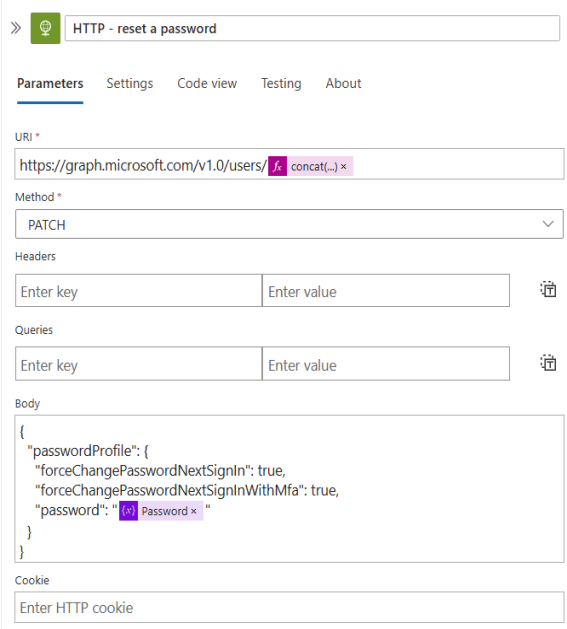


Kuva 9. Set variable satunnainen salasana (guid).

Toiminnon Set variable arvoon määritettiin substring(guid(), 0, 10) -lauseke, joka puolestaan tuottaa satunnaisen GUID-arvon (Globally Unique Identifier). Tässä tapauksessa muodostetaan 10-merkkinen arvo, jota voidaan hyödyntää käyttäjän väliaikaisena salasanana.

Satunnaisesti luotua salasanaa käytettiin HTTP-toiminnon Graph API -pyynnössä, joka vaihtaa käyttäjän salasanan. Käyttäjän salasanan nollaus toteutettiin Graph-rajapinnan

kautta hyödyntäen kuvan 10 mukaista osoitetta. HTTP-toiminnossa käytettiin PATCH-metodia, jolla voidaan päivittää käyttäjän tietoja.



Kuva 10. Käyttäjän salasanan vaihto (Reset password).

Salasanan nollauksen yhteydessä Microsoft Graph -rajapintaa käyttäen tehtiin myös erillisiä määrityksiä, kuten vaadi salasanan vaihto monivaiheisen tunnistautumisen kanssa, pakota salasanan vaihto seuraavan kirjautumisen yhteydessä sekä liitettiin aiemmin luotu satunnainen salasana muuttujasta (Password) käyttäjälle.

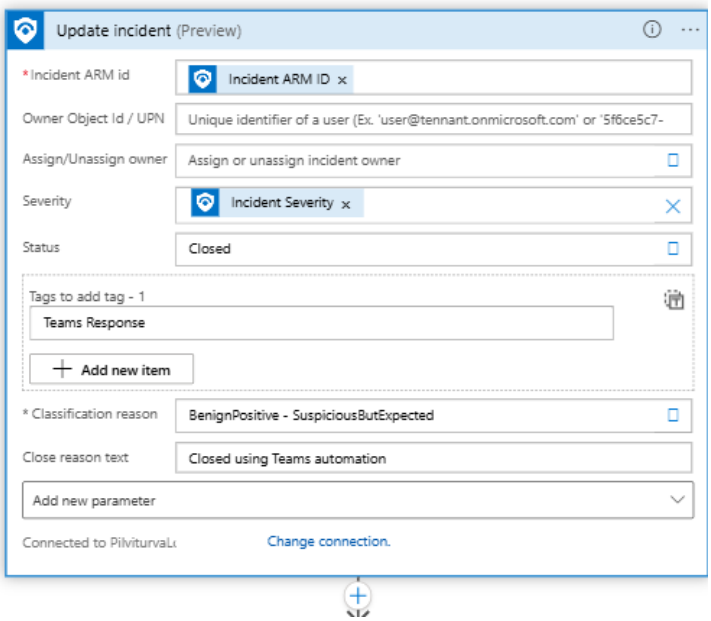
Salasanan nollaukseen käytetty Microsoft Graph -rajapinnan HTTP-pyyntö autentikoitiin hyödyntäen Logic Appin hallinnoitua identiteettiä (system-assigned managed identity), jolle määriteltiin PowerShellin kautta ”Password Administrator” -rooli (Microsoft, 2025h).

5.8 Microsoft Sentinel -hälytyksen sulkeminen mukautuvasta kortista

Mukautuvaan korttiin, joka lähetetään Microsoft Teamsin SOC-kanavalle lisättiin toiminto, jolla saatiin muutettua hälytys tilaan suljettu (Closed) Microsoft Sentinelistä. Näin se saatiin poistettua näkyvistä uusien hälytysten listalta Microsoft Sentinel -portaalista. Tämä toiminto on hyödyllinen etenkin, jos kyseessä on false-positive-hälytys tai hälytykseen liittyvä ratkaisu on saatu tehtyä ilman muita toimenpiteitä. Toimintoa suorittaessa tuli myös sulkea

alkuperäinen Microsoft Teamsiin lähetetty mukautuva kortti hälytyksestä, sillä hälytyksen tuplakäsittely aiheuttaa useimmin väärinkäsityksiä ja virheitä.

Logic Appin suunnittelutilassa (Logic App Designer) Microsoft Sentinel -toimintojen (actions) alla on valmiina toiminto Update incident, jonka avulla voidaan suorittaa Microsoft Sentinel -portaalin hälytyksen päivittäminen tilaan suljettu. Toiminnon tarkoituksena on sulkea Microsoft Sentinel -portaalista hälytys, kun mukautuvan kortin painiketta ”Close Incident” painetaan.

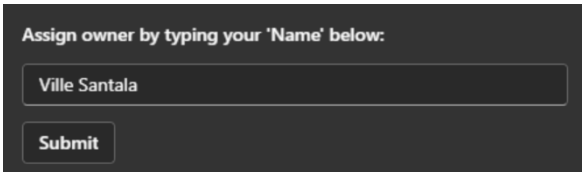


Kuva 11. Update Incident -toiminnon määritys.

Update Incident -toimintoon tehtiin seuraavat määritykset. Aiemmista vaiheista on haettu ”Incident Severity”, jota voidaan käyttää varmistamaan, että hälytys suljetaan samalla hälytyksen tasolla kuin se on tullut. Tilaan (Status) asetettiin ”Closed” ja luokittelun syyksi BenignPositive, sillä tässä tapauksessa haluttiin sulkea hälytys Microsoft Sentinelistä. Tähän osioon määriteltiin myös selvennykseksi tagi ”Teams Response”, joka kertoo, että hälytys on suljettu automaation kautta Microsoft Teamsista. Sulkemisen yhteydessä lisättiin ”Closed reason text”, joka kertoo, mitä kautta hälytys on suljettu. Microsoft Sentinelissä Incident ARM ID (Azure Resource Manager ID) on tapa yksilöidä ja viitata Microsoft Sentinel -hälytyksiin Azure-resurssina. Se on täysi Azure Resource Manager (ARM) -polku tiettyyn Microsoft Sentinel -hälytykseen (Microsoft, 2025a).

5.8.1 Nimen lisääminen hälytykseen

Sulkemisen yhteydessä lisättiin lisävahvistus, johon toiminnon suorittaja syöttää nimensä ja näin saadaan seurattua, kuka hälytyksen on käsitellyt. Vahvistuskenttään syötetty nimi lisättiin erikseen kommenttina hälytykseen Logic App -työnkulussa Add Comment -toiminnolla.



Kuva 12. Nimen lisääminen hälytykseen sulkemisen yhteydessä.

Käyttäjä syöttää nimensä kuvan 12 mukaisesti pyydettyyn lisävahvistuskenttään hänen painettua sulje hälytys -painiketta Microsoft Teamsiin saapuneesta mukautuvasta kortista. Käyttäjän painaessa Submit-painiketta, hälytys suljetaan sekä lisätään toiminnon suorittajan nimi hälytykseen kommenttina.

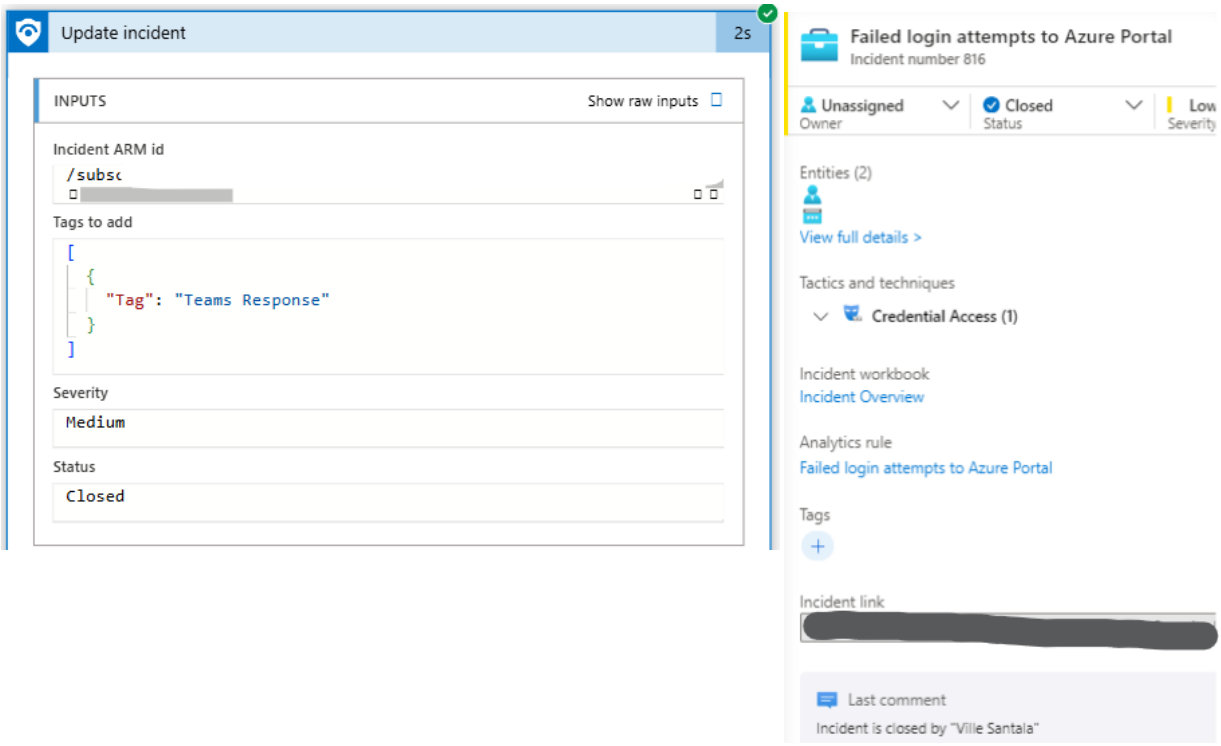
5.8.2 Update Incident -toiminnon suorittaminen

Hälytyksen sulkemistoimintoa ensimmäistä kertaa suorittaessa selvisi, että hälytyksen sulkeminen Microsoft Sentinel -portaalista Logic Appin ja mukautuvan kortin avulla edellyttää oikeanlaisia käyttöoikeuksia, ennen kuin se voidaan suorittaa onnistuneesti. Logic App -työnkulku päättyi ”Update Incident” -toiminnon virheilmoitukseen kuvan 13 mukaisesti, siinä mainitaan puuttuvista käyttöoikeuksista.

Kuva 13. Update Incident -toiminto, puuttuvat oikeudet virheilmoitus

Tämän toiminnon suorittamiseen tarvittiin ”Microsoft Sentinel Responder” -rooli, Logic Appia varten määritetylle hallitulle identiteetille (Managed Identity). Tarvittavat oikeudet, joita tarvittiin hälytyksen sulkemiseen ”Update Incident” -toiminnolla Microsoft Sentinelistä, löytyvät suoraan Microsoftin virallisesta dokumentaatiosta (Microsoft, 2024f).

Kun hallitulle identiteetille määriteltiin Microsoftin dokumentaatiossa mainittu ”Microsoft Sentinel Responder” -rooli, ja tätä hallittua identiteettiä käytettiin autentikoimaan ”Update Incident” -toiminto, saatiin suoritettua hälytyksen sulkeminen Logic App -työnkulun kautta onnistuneesti kuvan 14 mukaisesti Microsoft Sentinelistä.



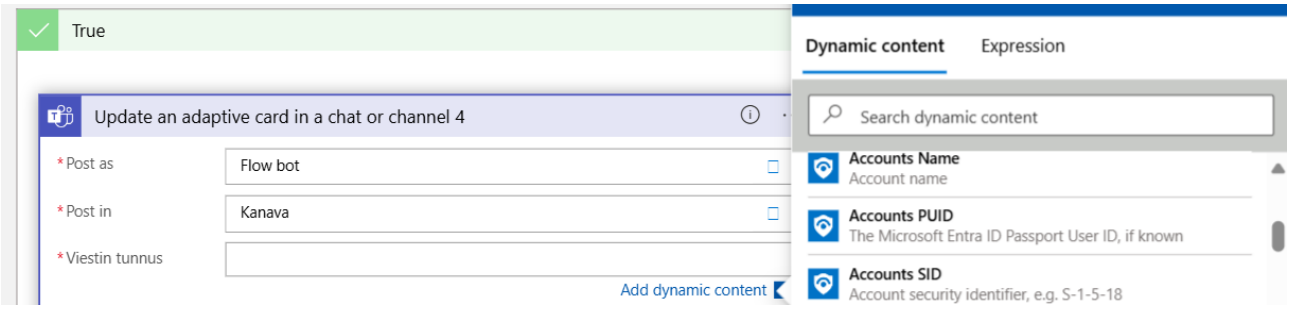
Kuva 14. Hälytyksen sulkeminen Sentinel-portaalista onnistuneesti.

5.9 Kortin hylkääminen

Logic App -työnkulun lähettämään mukautuvaan korttiin lisättiin myös toiminto, jolla voidaan sulkea pelkkä Microsoft Teamsiin lähetetty mukautuva kortti. Tämän toiminnon tarkoituksena on sulkea pelkästään Microsoft Teamsin SOC-kanavalle hälytyksestä lähetetty kortti ilman muita toimenpiteitä käyttäjätileihin tai laitteisiin liittyen. Kyseisellä toiminnolla saatiin hylättyä Microsoft Teamsissa aktiivisena oleva mukautuva kortti hälytyksestä,

jättäen kuitenkin alkuperäinen Microsoft Sentinel -hälytys edelleen New-tilaan Microsoft Sentinel -portaaliin.

Logic App -suunnittelutilassa Microsoft Teams -toimintoja tutkiessa selvisi, että kyseisen osion alla on valmiina toiminto (action), jolla pystyi päivittämään jo olemassa olevaa mukautuvaa korttia. Kyseinen toiminto oli nimellä Update adaptive card. Tällä toiminnolla pystyy korvaamaan alkuperäisen kortin Microsoft Teams -kanavalta, mukautuvan kortin yksilöityä tunnusta (messageId) hyödyntäen.



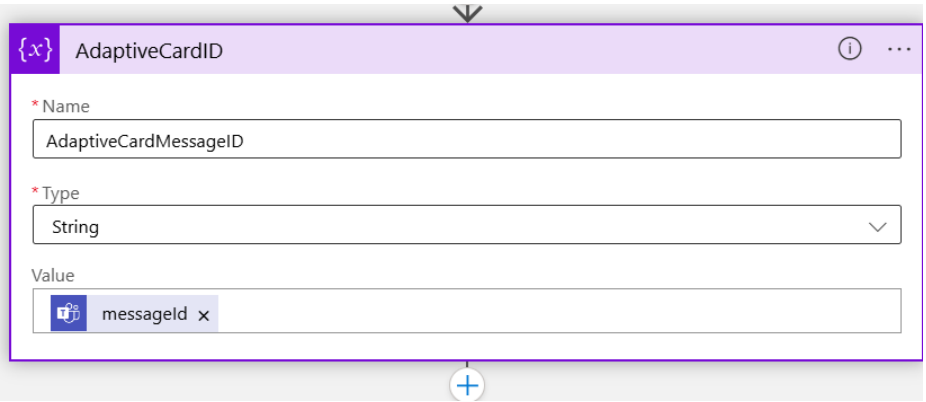
Kuva 15. Puuttuva viestin tunnus (messageId).

Kortin päivityksessä koitettiin viitata suoraan aiempien toimintojen sisällöstä mukautuvan kortin (messageId) arvoon kuvan 15 mukaisesti, mutta kyseistä arvoa ei löytynyt hakemalla. Arvoa ei ollut mahdollista käyttää suoraan, koska työnkulussa oltiin alempana eri osiossa ja määritelty kortti on Logic App -työnkulussa ylempänä.

5.9.1 Muuttuja tallentamaan mukautuvan kortin ID

Puuttuvalle (messageId) ongelmalle kehitettiin ratkaisuna erillinen muuttuja, johon lisättiin alkuperäisen mukautuvan kortin messageId, jotta sitä voitaisiin hyödyntää myöhemmin Logic App -työnkulussa. Logic App -työnkulussa alkuperäisen Post adaptive card in a chat or channel -toiminnon alle määriteltiin muuttuja Initialize variable, johon saatiin haettua suoraan alkuperäisen mukautuvan kortin tarvittava messageID-arvo kortin päivitystä varten. Muuttujalle annettiin sen tarkoitusta kuvaava nimi ja tyypiksi String sekä arvoon (Value) määritettiin expression-lauseke, jolla saatiin viitattua aiemman vaiheen mukautuvaan korttiin, ja haettua siitä tarvittava messageId:

- body('Post_adaptive_card_and_wait_for_a_response')['messageId']



Kuva 16. Mukautuvan kortin viestin tunnus (messageId).

Kyseinen lauseke noutaa kortin yksilöidyn tunnisteen (messageId) erikseen määritettyyn muuttujaan. Näin sitä voidaan hyödyntää myöhemmin kortin päivittämisessä.

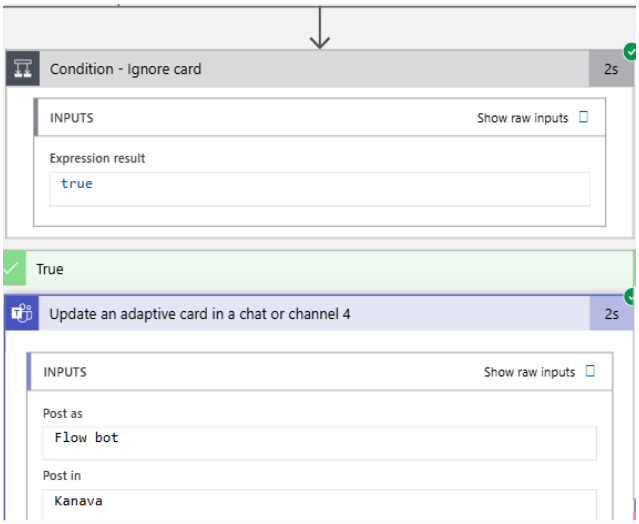
5.9.2 Toiminto suorittamaan mukautuvan kortin hylkäys Microsoft Teamsista

Logic App -suunnittelutilassa oli valmiina Microsoft Teams -toimintojen (actions) alla, Update an adaptive card in a chat or channel -toiminto, jolla pystyy korvata aiemmin määritetyn kortin käyttämällä mukautuvan kortin yksilöityä arvoa (messageId). Hälytyskortin poistaminen Microsoft Teams -kanavalta voitiin suorittaa suoraan kyseistä toimintoa ja aiemmin noudettua messageID-arvoa käyttäen.

Toimintoa voidaan hyödyntää tilanteissa, joissa hälytyksen jatkotoimenpiteitä ei katsota tarpeellisiksi, mutta Microsoft Teams -näkymä halutaan pitää siistinä ja ajantasaisena. Käytännössä Logic App -työnkulku tunnistaa alkuperäisen hälytyskortin yksilöidyn tunnisteen (messageId) avulla ja suorittaa kortin päivittämisen. Tämä lähestymistapa parantaa SOC-tiimin työskentelyn selkeyttä ja mahdollistaa yksinkertaisen tavan ilmaista, että kortti on käsitelty, vaikka hälytystä ei ole vielä virallisesti suljettu Microsoft Sentinel -portaalista.

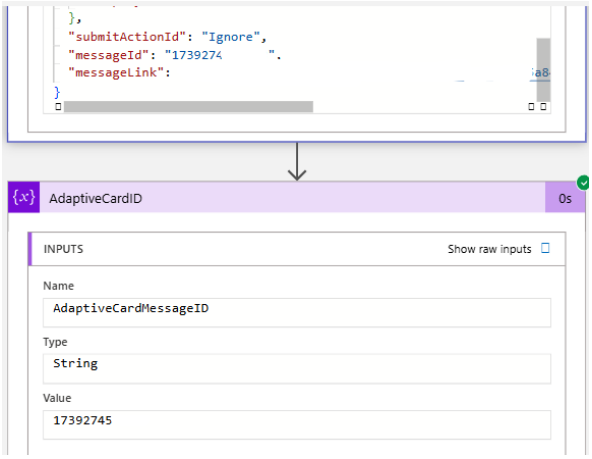
5.9.3 Toiminnon suorittaminen

Toimintoa testattaessa suoritettiin Microsoft Teamsin SOC-kanavalle tulleesta mukautuvasta kortista toiminto hylkää (Ignore), jonka myötä kortti korvattiin onnistuneesti Update Adaptive Card -toiminnon avulla uudella kortilla sekä poistettiin samalla alkuperäinen kortti.



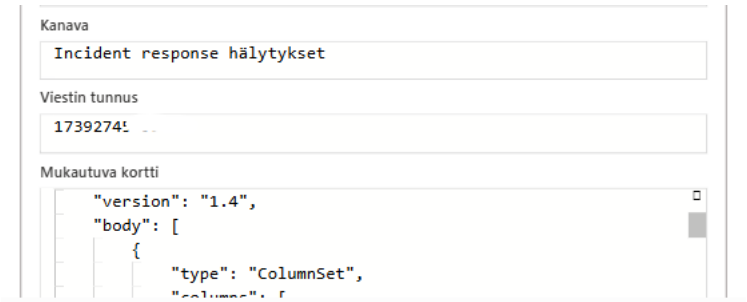
Kuva 17. Hälytyskortin korvaus Microsoft Teams -kanavalta.

Tässä tapauksessa suoritettiin toiminto ”Ignore Card” eli siirryttiin ehtolausekkeen ”Condition – Ignore card” vaiheissa eteenpäin. Ehtolauseke tarkistaa, mitä painiketta mukautuvasta kortista on painettu, ja etenee sen myötä oikeasta vaiheesta eteenpäin. Molemmat vaiheet suoritettiin onnistuneesti kuvan 17 mukaisesti.



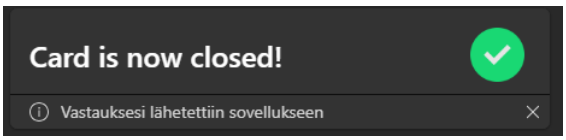
Kuva 18. ”Ignore”-toiminnon suoritus Logic Appista.

Logic App tunnisti toiminnon, jonka ID on määritelty mukautuvan kortin rakenteessa ”Ignore”-nimellä kuvan 18 mukaisesti. Toiminto suoritettiin ja haettiin aiemmin työnkulussa määritettyyn muuttujaan mukautuvan kortin messageID-arvo. Kyseinen arvo toimii tunnisteena, jonka avulla Logic App -työnkulku osaa kohdistaa oikean kortin jatkokäsittelyä varten. Tällainen rakenne mahdollistaa useiden korttien samanaikaisen hallinnan, sillä jokainen kortti voidaan yksilöidä hyödyntämällä kortin messageID-arvoa ja käsitellä omana kokonaisuutenaan ilman ristiriitoja. Tämä parantaa ylläpidettävyyttä myös laajemmassa käytössä.



Kuva 19. Vastaus Update Adaptive Card -toiminnosta.

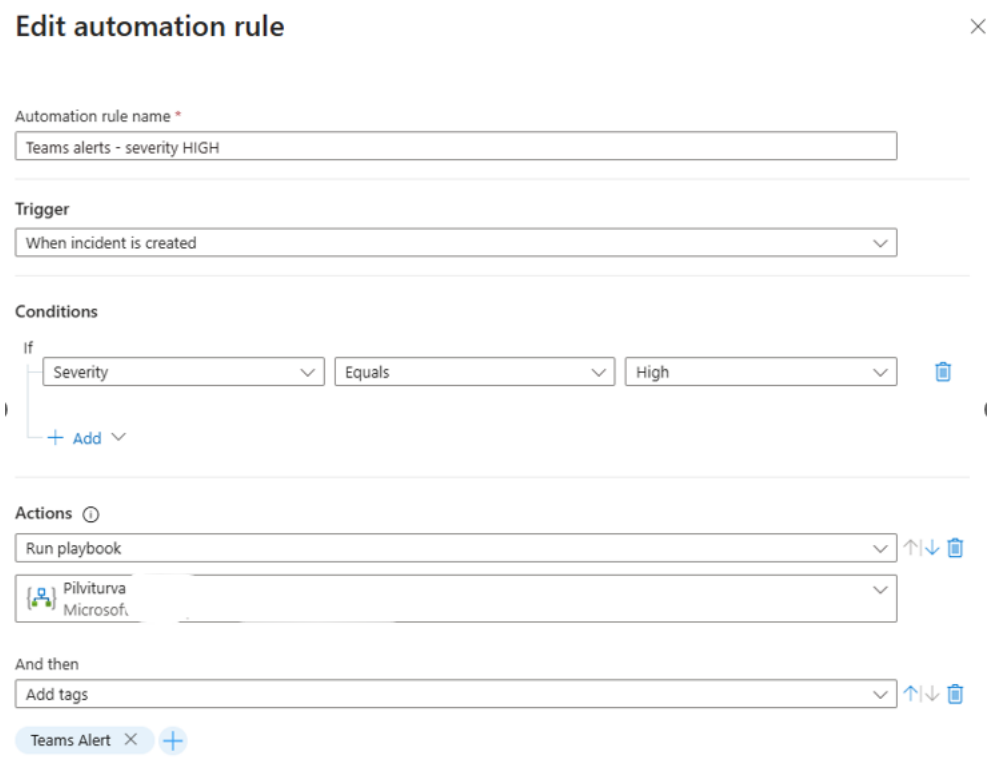
Toiminnossa, joka suorittaa kortin sulkemisen (Update adaptive card), käytettiin aiemmin erilliseen muuttujaan lisättyä alkuperäisen kortin yksilöityä messageID-arvoa. Toimintoon, joka päivittää alkuperäisen kortin, on määritelty mukautuvan kortin suunnittelutyökalulla Adaptive Card Designer rakenne, joka on kuvattuna kuvassa 20. Kyseinen palaute tulee Microsoft Teamsin SOC-kanavalle, kun nappia ”Ignore Card” on painettu.



Kuva 20. Palautettu tulos ”Ignore”-toiminnosta Microsoft Teams -kanavalle.

5.10 Automaatiosäännön toteuttaminen

Toteutukseen tarvittiin myös automaatiosääntö, jotta luotu Logic App käynnistyy automaattisesti, mikäli siihen määritetyt ehdot täyttyvät. Automaatiosäännön luominen oli helpoin osio koko prosessista, sillä sen määrittäminen oli todella suoraviivaista ja yksinkertaista. Automaatiosääntö luotiin suoraan aktiivisesta Microsoft Sentinel -näkymän ”Automation”-osiosta. Osiosta valittiin yläreunasta ”Create” ja sen alta vaihtoehto ”Automation rule”.



Kuva 21. Automaatiosäännön määritys.

Automaatiosääntöön määriteltiin kuvan 21 mukainen ehto, eli jos Microsoft Sentineliin saapuneen hälytyksen vakavuustaso (Severity) vastaa automaatiosäännön ehtoon määritettyä ”HIGH”-arvoa, käynnistetään sääntöön liitetty Logic App -automaatio.

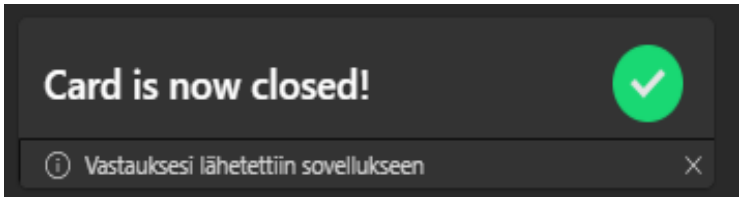
Muita automaatiosäännön ominaisuuksia tutkiessa selvisi, että automaatiosääntöön olisi mahdollista myös rajata, mitkä Microsoft Sentinel -analytiikat käsitellään kyseisen automaation avulla. Seuraavanlaista ratkaisua voitaisiin hyödyntää tilanteissa, jossa luotu Logic App -automaatio käsittelee vain tietyn Microsoft Sentinel -analytiikan tuottamat hälytykset -ja toteuttaa tietyt toimenpiteet.

6 TULOKSET

Lopputestauksessa kaikki toimenpiteet suoritettiin onnistuneesti, ja niiden osalta saavutettiin sekä odotetut tulokset että ennalta määritetyt tavoitteet.

6.1 Vastaus ”Ignore”-toiminnolle

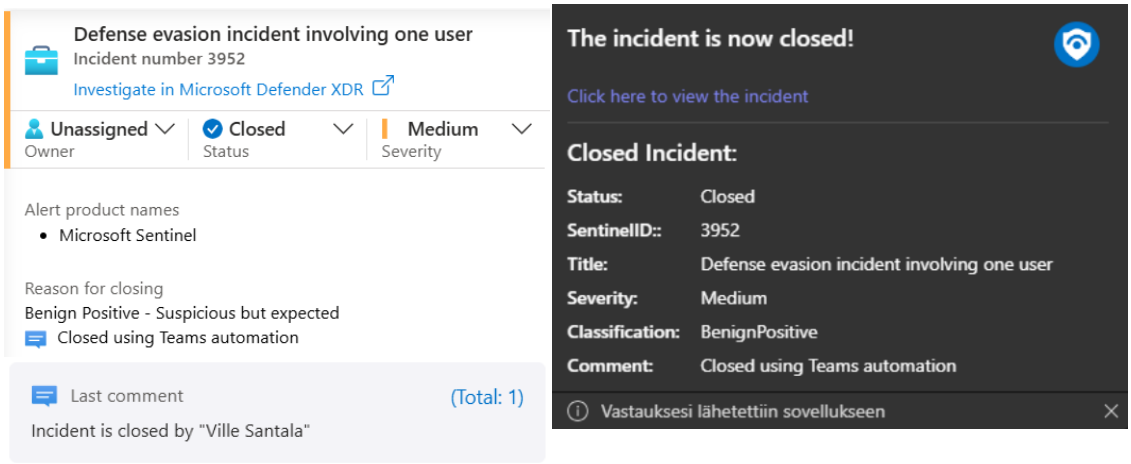
Kortin hylkääminen Microsoft Teams -kanavalta suoritettiin onnistuneesti. Logic App -työnkulku katkaistiin suoritetun toimenpiteen jälkeen ja Microsoft Teams -kanavalle lisättiin kuvan 22 mukainen palaute. Muita toimenpiteitä ei suoritettu tämän toimenpiteen yhteydessä.



Kuva 22. Palautus Ignore-toiminnosta.

6.2 Vastaus ”Close Incident” -toiminnolle

Microsoft Sentinel -hälytyksen sulkeminen mukautuvasta kortista suoritettiin myös odotetusti Microsoft Teams -kanavalta kuvan 23 mukaisesti.

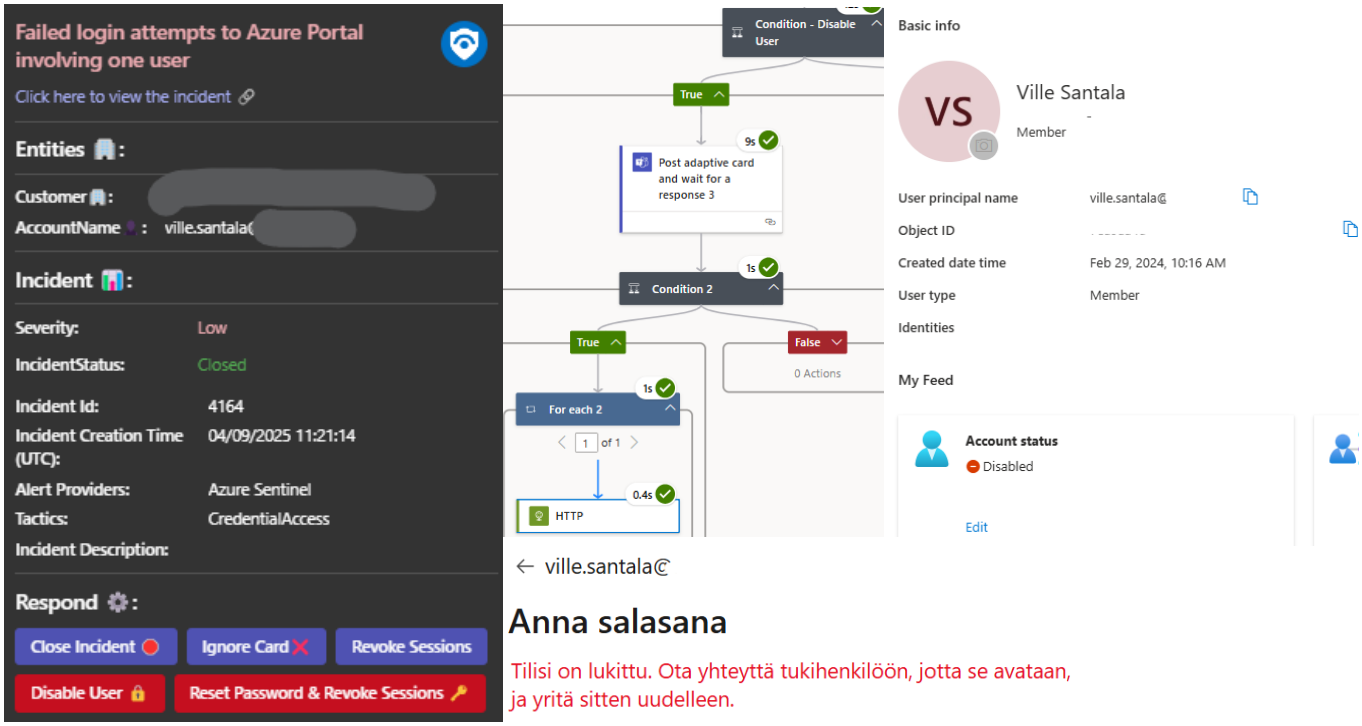


Kuva 23. Palaute Close Incident -toiminnosta.

Toiminto suoritti hälytyksen sulkemisen Microsoft Sentinel -portaalista hyödyntäen tarvittavia käyttöoikeuksia sekä lähetti tästä ilmoituksen Microsoft Teams -kanavalle. Logic App -automaatio lisää kommenttina hälytykseen myös tiedon, kuka on sulkenut kyseisen hälytyksen.

6.3 Vastaus ”Disable User” -toiminnolle

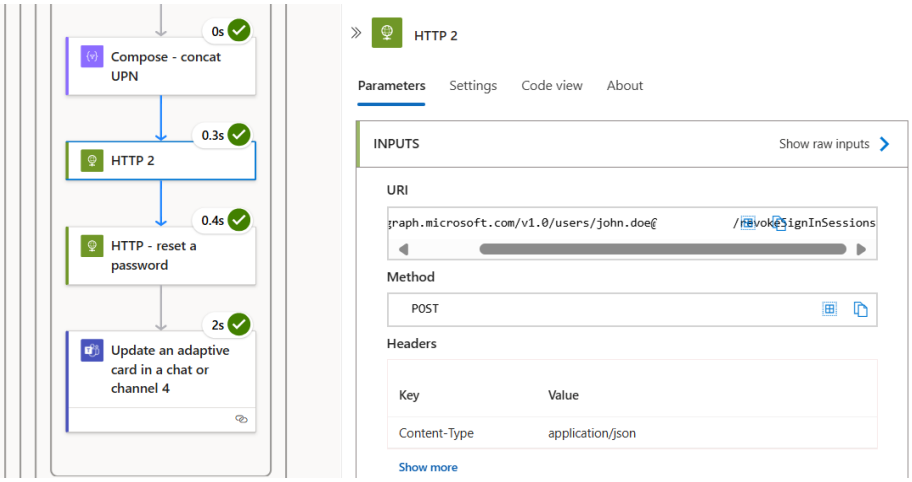
Toiminto, jolla käyttäjän kirjautuminen voidaan estää, suoritettiin onnistuneesti kuvan 24 mukaisesti. Korttiin määritettyä ”Disable”-toimintoa suoritettaessa edellytettiin lisävahvistusta, jolla varmistettiin, haluaako käyttäjä todella suorittaa toimenpiteen kyseiselle tunnukselle. Vahvistuksen jälkeen mukautuva kortti suljetaan Microsoft Teams -kanavalta ja hälytyksessä ollut käyttäjä asetetaan ”Disabled”-tilaan Microsoft Entra ID:stä.



Kuva 24. Onnistunut suoritus "Disable"-toiminnosta.

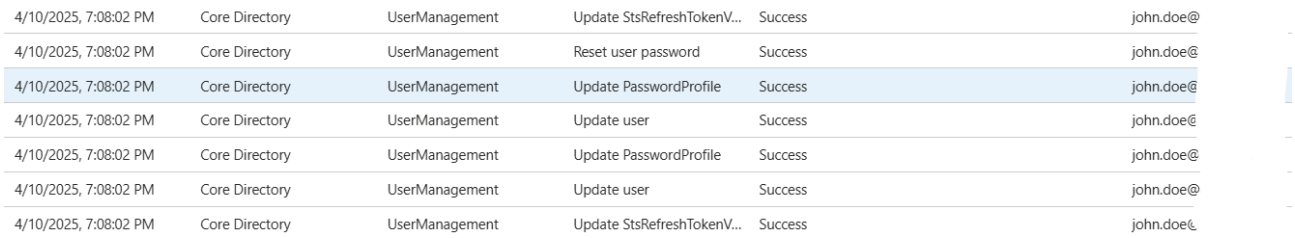
6.4 Vastaus “Reset Password & Revoke Sessions” -toiminnolle

Toiminto, jolla käyttäjän aktiiviset istunnot ja salasana nollattiin, suoritettiin kokonaisuudessaan onnistuneesti. Istunnot nollattiin onnistuneesti kuvan 25 mukaisesti, mutta tästä ei lähetetty erillistä palautetta Microsoft Teams -kanavalle.



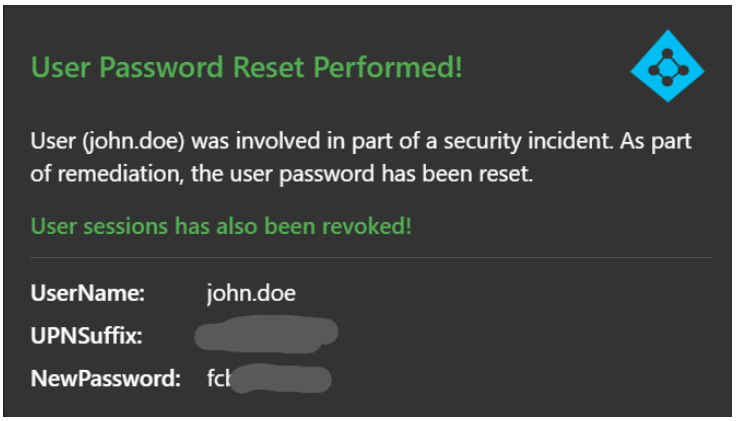
Kuva 25. Onnistunut käyttäjän istuntojen uusiminen (Revoke) Logic App -työnkulusta.

Logic Appin kautta suoritetun ”Revoke”-toiminnon onnistunut suoritus tarkistettiin vielä Microsoft Entra ID:n Audit Logs -osiosta kuvan 26 mukaisesti. Samalla tarkistettiin, onnistuiko käyttäjän salasanan nollaus.



Kuva 26. Onnistunut istuntojen ja salasanan nollaus Microsoft Entra ID:n Audit Logs -osiosta.

Käyttäjälle luotiin GUID-arvon (Globally Unique Identifier) avulla 10-merkkinen väliaikainen salasana, joka palautettiin Microsoft Teams -kanavalle kuvan 27 mukaisesti, josta se voitiin edelleen välittää asiakkaalle.



Kuva 27. Uuden salasanan palautus Microsoft Teams -kanavalle.

Loppukäyttäjä syöttää SOC-analyytikon lähettämän, Logic App -työnkulun kautta luodun väliaikaisen salasanan ja määrittää tilalle haluamansa salasanan.

Kuva 28. Uuden salasanan määritys nollauksen jälkeen.

Graph-rajapinnan kautta lähetettyyn pyyntöön on määritetty asetukset "forceChangePasswordNextSignIn": true ja "forceChangePasswordNextSignInWithMfa": true. Tämän seurauksena käyttäjältä vaaditaan salasanan vaihto ensimmäisellä kirjautumiskerralla monivaiheisen tunnistautumisen yhteydessä kuvan 28 mukaisesti.

7 JOHTOPÄÄTÖKSET

Opinnäytetyössä toteutettiin automaatioratkaisu Microsoft Sentinel -hälytysten rinnalle hyödyntäen Azure Logic Apps- ja Adaptive Cards -teknologiaa. Työn tavoitteena oli tehostaa ja helpottaa SOC-tiimin työskentelyä mahdollistamalla Microsoft Sentinel -tietoturvahälytysten käsittely suoraan Microsoft Teamsiin lähetystä mukautuvasta kortista (Adaptive Card) ja vähentää manuaalista SOC-tiimin työkuormaa.

Automaatio saatiin toteutettua onnistuneesti, ja se täytti sille asetetut tavoitteet. Microsoft Sentinelistä Teamsiin lähetetyn mukautuvan kortin avulla voitiin suorittaa keskeisiä toimenpiteitä, kuten kortin hylkääminen Microsoft Teamsissa, käyttäjän kirjautumisen estäminen, salasanan ja istuntojen nollaaminen sekä hälytyksen sulkeminen Microsoft Sentinel -portaalista.

Automaatioratkaisua ja sen toimintaa on testattu Microsoft Sentinel -hälytyksillä testiympäristössä, joka on erillään asiakasympäristöistä.

Toteutetun ratkaisun suurimpana hyötynä voidaan pitää sen kykyä tehostaa SOC-tiimin työskentelyä ja lyhentää vasteaikaa kriittisiin hälytyksiin. Tavoitteena ollut automaatioratkaisun kehittäminen SOC-tiimin käyttöön saavutettiin onnistuneesti, ja toimeksiantajalle tarjottiin konkreettinen malli, jota voidaan hyödyntää ja laajentaa tulevaisuudessa. Ratkaisua voidaan jatkossa soveltaa, mukauttaa ja hyödyntää myös muihin hälytystyyppeihin ja prosesseihin.

Vaikka automaatioratkaisu toimi suunnitellusti, kehitystyön aikana havaittiin myös haasteita, erityisesti käyttöoikeuksien hallinnassa, HTTP-toimintojen määrittelyssä ja lausekkeiden (expressions) toteuttamisessa.

Haasteita käydään läpi erikseen ”Haasteita” -osiossa.

8 POHDINTA, HAASTEET JA KEHITYSMAHDOLLISUUDET

Lopputuloksena tätä ratkaisua toteuttaessa sekä muita ratkaisuja tutkiessa ja testatessa huomattiin, kuinka käytännöllisiä Microsoft Logic Appit ovat. Logic App -työnkulkuja voi käyttää tehokkaasti SOC-tiimin tukena helpottamaan, tehostamaan ja nopeuttamaan päivittäisiä prosesseja. Täysin manuaalisella lähestymistavalla vasteaika hälytyksiin on korkeampi, ellei tähän määritetty työntekijä ole erikseen valvomassa hälytyksiä jatkuvasti Microsoft Sentinel -portaalissa. Ilman automaatioita hälytysten määrä on oletettavasti suurempi, eli hälytyksiä nousee väistämättä enemmän. Tämä ero korostuu tilanteissa, joissa tulosten karsintaa on tehostettu esimerkiksi lisäämällä luotettujen ja haitallisten osoitteiden suodattimia sekä liittämällä taustalle automaattisia toimenpiteitä ja ilmoituksia.

Toteutetulla ratkaisulla voidaan toteuttaa toimenpiteitä ainoastaan oman ympäristön käyttäjille, mutta tähän kehitettiin ratkaisu, jolla voidaan toteuttaa toimenpiteitä Graph-rajapinnan avulla myös eri käyttöympäristössä (tenant) sijaitsevien asiakkaiden käyttäjille. Toteutettua lisälogiikkaa käydään läpi erikseen jatkokehitys-osiossa.

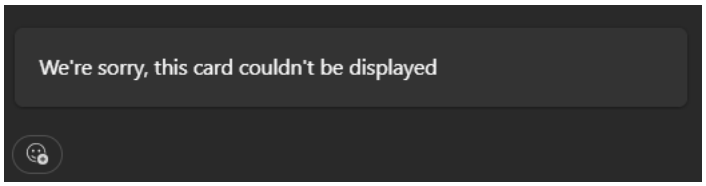
8.1 Haasteita

Erikseen Logic Appin -toimintoihin määritetyiden lausekkeiden kanssa (Expression) kanssa esiintyi ongelmia ja haasteita. Expression-lausekkeet ovat dynaamisia kaavoja, joita käytetään Microsoft Logic Apps -työnkuluissa tietojen käsittelyyn ja muokkaamiseen ja ne mahdollistavat esimerkiksi arvojen muuntamisen, tietojen suodattamisen ja ehtoihin perustuvat päätökset ilman erillistä koodia (Microsoft, 2025i). Oikeanlaisten lausekkeiden toteuttamisessa ilmeni ongelmia aluksi, etenkin mukautuvien korttien painikkeiden ja halutun sisällön hakemisessa korttiin onneksi kuitenkin Microsoftin virallisesta dokumentaatiosta löytyi apua viittauksiin.

Toteutetuissa mukautuvissa korteissa (Adative Cards) huomioitiin muutamia teknisiä esteitä, kuten takaisin-toiminnon suorittaminen kortteihin eli mukautuviin kortteihin ei ollut mahdollista toteuttaa peruutustoimintoa, jolla pääsisi kortissa edelliseen vaiheeseen. Käytännössä takaisin-vaiheen puute voi aiheuttaa tilanteen, jossa hälytyksen tarkastelija on ehtinyt painaa esimerkiksi toimintoa, joka sulkee käyttäjän tilin tilapäisesti ja on siirtynyt

työnkulussa toiminnon vahvistamiseen, mutta hän ei pääse enää kortissa taaksepäin ja joutuu käsitellä hälytyksen Microsoft Sentinel -portaalin kautta.

Mukautuvien korttien JSON-rakennetta liitettäessä Logic Appin -työnkulussa toimintoon, joka lähettää kortin Microsoft Teams -kanavalle, huomattiin myös kortin version kanssa ongelmia. Ongelmia ilmeni erityisesti, kun kortti luodaan mukautuvien korttien suunnittelualustalla (Adaptive Card Designer). Kortti käyttää oletuksena versiota 1.6, joka ei toiminut suoraan Microsoft Teamsissa vaan saatiin ainoastaan kuvan 29 mukainen ilmoitus, että kortin sisältöä ei voida näyttää.



Kuva 29. Virheilmoitus mukautuvan kortin versiosta.

Ongelma saatiin kuitenkin korjattua käyttämällä aiempaa versiota 1.4, jonka jälkeen hälytyskortit näkyivät Microsoft Teams -kanavalla normaalisti.

Ongelmia ilmeni myös puutteellisten käyttöoikeuksien vuoksi, sillä jokainen käyttöoikeuden lisääminen Logic Appin hallitulle identiteetille tai sitä varten luodulle rekisteröidylle sovellukselle (App registration) vaati erillisen henkilön, joka lisäsi oikeudet manuaalisesti. Tämän jälkeen vasta voitiin testata Logic App -työnkulun toimintoja ja korjata mahdollisia virheitä. Tämä aiheutti Logic Appin toteuttamisessa ja testaamisessa jonkin verran viiveitä.

8.2 Jatkokehitys

Logic App -automaatioon rakennettiin lisälogiikka, joka hakee asiakkaan käyttöympäristöön (tenant) automaatiota varten luodun rekisteröidyn sovelluksen (App registration) tunnistetiedot. Toteutettu logiikka hyödyntää Logic Appin työnkulussa Azure Key Vaultia, joka on pilvipalvelu turvalliseen tietojen, kuten asiakkaan sovelluksen client ID- ja client secret -arvojen, säilyttämiseen (Microsoft, 2025k). Näitä arvoja käytettiin toimenpiteiden suorittamiseen oikean asiakkaan ympäristössä hyödyntäen tenantID-arvoa asiakkaan tarkistukseen. Azure Key Vaultiin tallennetut tunnistetiedot mahdollistavat toimenpiteiden toteuttamisen Graph API:n kautta asiakkaan tenantissa oleville käyttäjille.

Logic Appia varten luodulle (App registration) sovellukselle myönnetään tarvittavat oikeudet asiakkaan ympäristöön määritettyjen toimenpiteiden suorittamiseen, kuten istuntojen uusimiseen, salasanan nollaamiseen ja käyttäjän kirjautumisen estämiseen. Tämän lisälogiikan keskeinen tarkoitus on hakea Azure Key Vaultista asiakkaan sovelluksen client ID- ja client secret -arvot, joita hyödynnetään autentikointitunnuksen hakemiseen. Tämän tunnuksen avulla suoritetaan varsinainen toimenpide käyttäjälle asiakkaan ympäristössä.

Yhtenä jatkokehitysideoista esiin nousee automaation laajentaminen kattamaan laajemmin SOC-toimintoja. Logic App -automaatioita voitaisiin hyödyntää hälytysten rikastamiseen kolmansien osapuolten rajapintojen, kuten VirusTotalin tai muiden kustannustehokkaampien ratkaisujen avulla. SOC-automaatioissa on kuitenkin suositeltavaa, että Logic App -automaatioita eriytetään, että yksittäisen työnkulun koko ei kasva liialliseksi.

Toteutuksen rinnalle voidaan rakentaa uusia, itsenäisiä Logic App -työnkulkuja, jotka suorittavat yksittäisiä toimenpiteitä kuten käyttäjän istuntojen uusimista, vaarantuneen käyttäjän kirjautumisen estämistä tai salasanan uusimista. Tässä on tärkeää huomioida, että automaatioihin liitettävän Microsoft Sentinel -analytiikan on oltava tarkkaa, sillä virheellisesti suoritettu vastatoimenpide voi aiheuttaa haittaa ja hämmennystä käyttäjille.

Automaation avulla voidaan toteuttaa suoria vastatoimenpiteitä tiettyihin Microsoft Sentinel -analytiikoihin määritettyihin hälytyksiin heti, kun hälytys syntyy. Tämä on erityisen hyödyllistä organisaatioissa, joissa ei ole käytössä ympärivuorokautista SOC-valvontaa. Lisäksi Logic App -automaatioita voidaan hyödyntää vähentämään tarpeettomien hälytysten määrää, joita jotkut analytiikat saattavat aiheuttaa. Odotettujen ja samoilla tiedoilla toistuvien hälytysten käsittely manuaalisesti kuormittaa SOC-tiimin työntekijöitä. Tällaisiin hälytyksiin on järkevä käyttää automaatioita.

Tässä yhteydessä myös analytiikan personointi on järkevää. Hälytyksen toistuessa usein samasta lähteestä odotetuilla tiedoilla voidaan harkita kyseisten tietojen poisjättämistä analytiikan kyselyrakenteesta, jolloin vältetään turhat hälytykset.

LÄHTEET

Asiakastieto. (i.a). *Databros Services Oy.* Asiakastieto. Databros Services Oy - Taloustiedot | Suomen Asiakastieto Oy

Cross, K. (24.3.2024). *SOC automation*. CrowdStrike. https://www.crowdstrike.com/en-us/cybersecurity-101/next-gen-siem/soc-automation/

Gruner, E. (9.7.2024). *IBM QRadar: Key Modules, Features, Architecture, and Limitations*. Cynet. https://www.cynet.com/siem/ibm-qradar-key-modules-features-architecture-and-limitations/

IBM. (9.4.2024a). *What is an API (application programming interface)?* IBM. https://www.ibm.com/topics/api

IBM. (15.3.2024b). *What is a security operations center (SOC)?* IBM. https://www.ibm.com/think/topics/security-operations-center

IBM. (i.a.-a). *IBM QRadar SIEM – Product overview*. https://www.ibm.com/products/qradar-siem

IBM. (i.a.-b). *IBM QRadar on Cloud – Data sheet*. https://www.ibm.com/downloads/cas/YD7JER5N

Microsoft. (i.a.-a). *Microsoft Sentinel – Cloud-native SIEM solution*. https://azure.microsoft.com/en-us/products/microsoft-sentinel/

Microsoft. (i.a.-b). *Microsoft Sentinel pricing*. https://azure.microsoft.com/en-us/pricing/details/microsoft-sentinel/

Microsoft. (i.a.-c). *What is Azure?* Microsoft Azure. https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-azure

Microsoft. (i.a.-d). *What is SIEM?* Microsoft Security. https://www.microsoft.com/en-us/security/business/security-101/what-is-siem#What-is-SIEM

Microsoft. (i.a.-e). *What is SOAR? Technology and solutions*. Microsoft Security. https://www.microsoft.com/en-us/security/business/security-101/what-is-soar

Microsoft. (i.a.-f). *What is a security operations center (SOC)?* Microsoft Security. https://www.microsoft.com/en-us/security/business/security-101/what-is-a-security-operations-center-soc

Microsoft. (i.a.-g). *Action.Submit*. Adaptive Cards Schema Explorer. https://adaptivecards.io/explorer/Action.Submit.html

Microsoft. (10.3.2021). *Overview of Adaptive Cards*. Microsoft Learn. https://learn.microsoft.com/en-us/adaptive-cards/

Microsoft. (6.5.2022). *Using Microsoft Teams Adaptive Cards to enhance incident response in Microsoft Sentinel*. Microsoft Tech Community. Using Microsoft Teams Adaptive Cards to enhance incident response in Microsoft Sentinel | Microsoft Community Hub

Microsoft. (8.9.2023). *Overview of adaptive cards for Microsoft Teams*. Microsoft Learn. https://learn.microsoft.com/en-us/power-automate/overview-adaptive-cards

Microsoft. (16.10.2024a). *Automate threat response in Microsoft Sentinel with automation rules*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/sentinel/automate-incident-handling-with-automation-rules?tabs=onboarded

Microsoft. (19.11.2024b). *Create, manage, and use automation rules in Microsoft Sentinel*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/sentinel/create-manage-use-automation-rules?tabs=azure-portal%2Conboarded

Microsoft. (19.11.2024c). *Threat detection in Microsoft Sentinel*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/sentinel/threat-detection

Microsoft. (21.5.2024d). *What is Microsoft Sentinel?* Microsoft Learn. https://learn.microsoft.com/en-us/azure/sentinel/overview?tabs=azure-portal

Microsoft. (23.12.2024e). *Use a Microsoft Sentinel playbook to stop potentially compromised users*. Microsoft Learn. https://docs.azure.cn/en-us/sentinel/automation/tutorial-respond-threats-playbook

Microsoft. (24.12.2024f). *Update Incident*. Microsoft Learn. https://learn.microsoft.com/en-us/graph/api/security-incident-update?view=graph-rest-1.0&tabs=http

Microsoft. (31.10.2024g). *Microsoft now a Leader in three major analyst reports for SIEM.* Microsoft Tech Community. https://techcommunity.microsoft.com/blog/microsoft-security-blog/microsoft-now-a-leader-in-three-major-analyst-reports-for-siem/4278853?utm_source=chatgpt.com

Microsoft. (30.7.2024h). *Plan costs and understand Microsoft Sentinel pricing and billing*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/sentinel/billing?tabs=simplified%2Ccommitment-tiers#free-data-sources

Microsoft. (1.4.2025a). *Azure Resource Manager documentation*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/azure-resource-manager/management/overview

Microsoft. (11.1.2025b). *Update user*. Microsoft Learn. https://learn.microsoft.com/en-us/graph/api/user-update?view=graph-rest-1.0&tabs=http

Microsoft. (29.1.2025c). *What is Azure Logic Apps?*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/logic-apps/logic-apps-overview

Microsoft. (3.4.2025d). *Designing Adaptive Cards for your Microsoft Teams app*. Microsoft Learn. https://learn.microsoft.com/en-us/microsoftteams/platform/task-modules-and-cards/cards/design-effective-cards?tabs=design

Microsoft. (18.3.2025e). *user: revokeSignInSessions.* Microsoft Learn. https://learn.microsoft.com/en-us/graph/api/user-revokesigninsessions?view=graph-rest-1.0&tabs=http

Microsoft. (27.3.2025f). *What are connectors in Azure Logic Apps*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/connectors/introduction

Microsoft. (16.2.2025g). *Build a workflow with a trigger or action in Azure Logic Apps*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/logic-apps/create-workflow-with-trigger-or-action?tabs=consumption

Microsoft. (8.1.2025h). *Microsoft Entra built-in roles*. Microsoft Learn. https://learn.microsoft.com/en-us/entra/identity/role-based-access-control/permissions-reference

Microsoft. (27.3.2025i). *Reference guide to workflow expression functions in Azure Logic Apps and Power Automate*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/logic-apps/workflow-definition-language-functions-reference

Microsoft. (11.4.2025j). *What are managed identities for Azure resources?* Microsoft Learn. https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/overview

Microsoft. (15.4.2025k). *Azure Key Vault basic concepts*. Microsoft Learn. https://learn.microsoft.com/en-us/azure/key-vault/general/basic-concepts

Microsoft. (5.3.2025l). *What is Microsoft Entra ID?* Microsoft Learn. https://learn.microsoft.com/en-us/entra/fundamentals/whatis

Palo Alto Networks. (i.a.). *What is SOAR?* Palo Alto Networks. https://www.paloaltonetworks.com/cyberpedia/what-is-soar

Pejman, J. (8.8.2022). *IBM QRadar: Security information and event management (SIEM)*. https://jubinpejman.com/ibm-qradar-security-information-and-event-management-siem/

Riyani, N. (8.9.2024). *Designing adaptive cards for Microsoft Teams*. LinkedIn. https://www.linkedin.com/pulse/designing-adaptive-cards-microsoft-teams-nadir-riyani-6eosf

Robb, D. (5.10.2018). *Splunk Enterprise Security Review: SIEM Product Features & Pricing*. eSecurity Planet. https://www.esecurityplanet.com/products/splunk-enterprise-security-es/

Splunk. (i.a.-a). *Splunk Enterprise Security – Analytics-driven SIEM*. https://www.splunk.com/en_us/products/enterprise-security.html

Splunk. (i.a.-b). *Splunkbase apps and add-ons*. https://splunkbase.splunk.com/

Tietokeskus. (i.a.). *Databros on nyt Tietokeskus*. https://www.tietokeskus.fi/databros-on-nyt-tietokeskus/