Atea Sentinel Pilotti ja kehitys

Microsoft Sentinel SIEM -ratkaisu

Etu sukunimi
Etu.suku@atea.fi

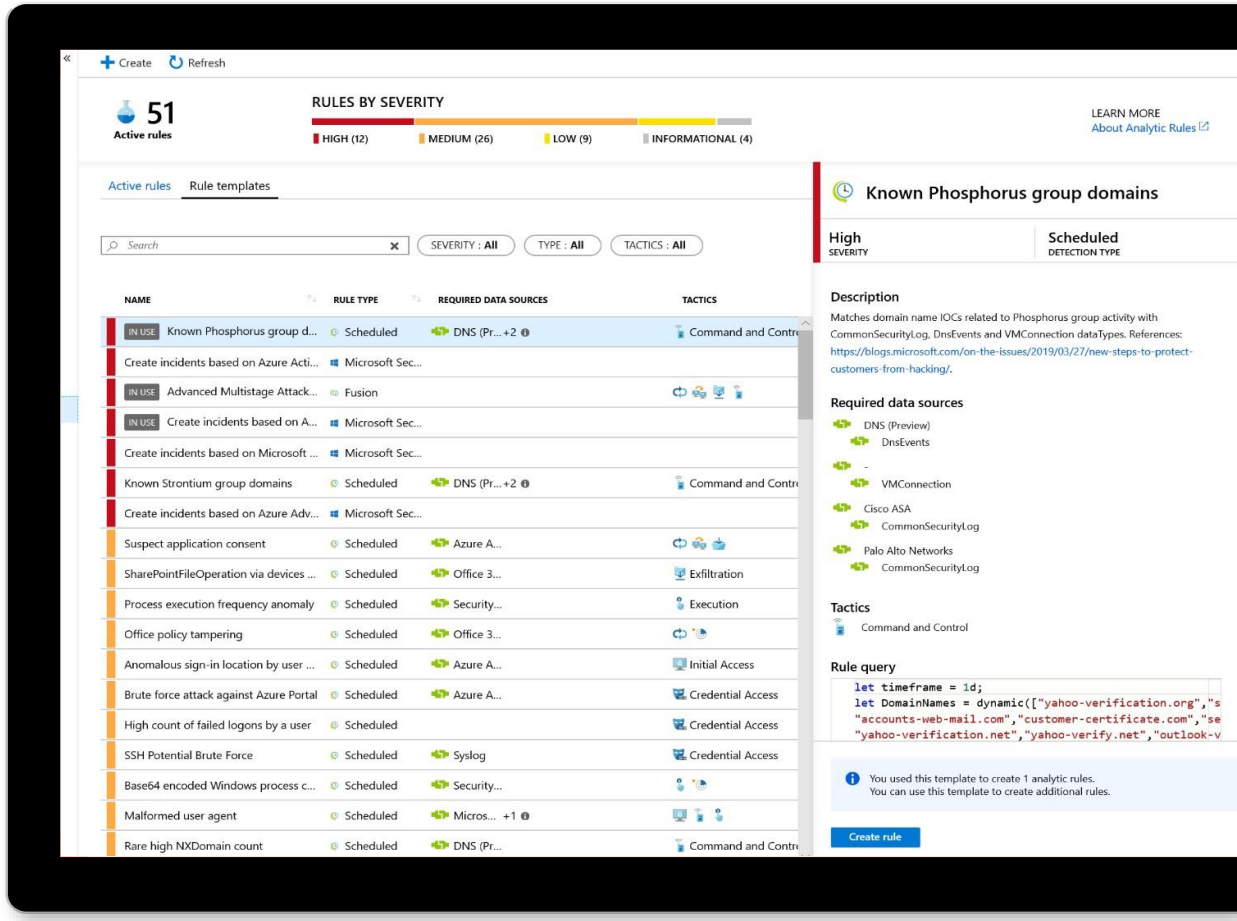
Keskitetyn logien hallinnan hyödyt

Helppo ja suoraviivainen

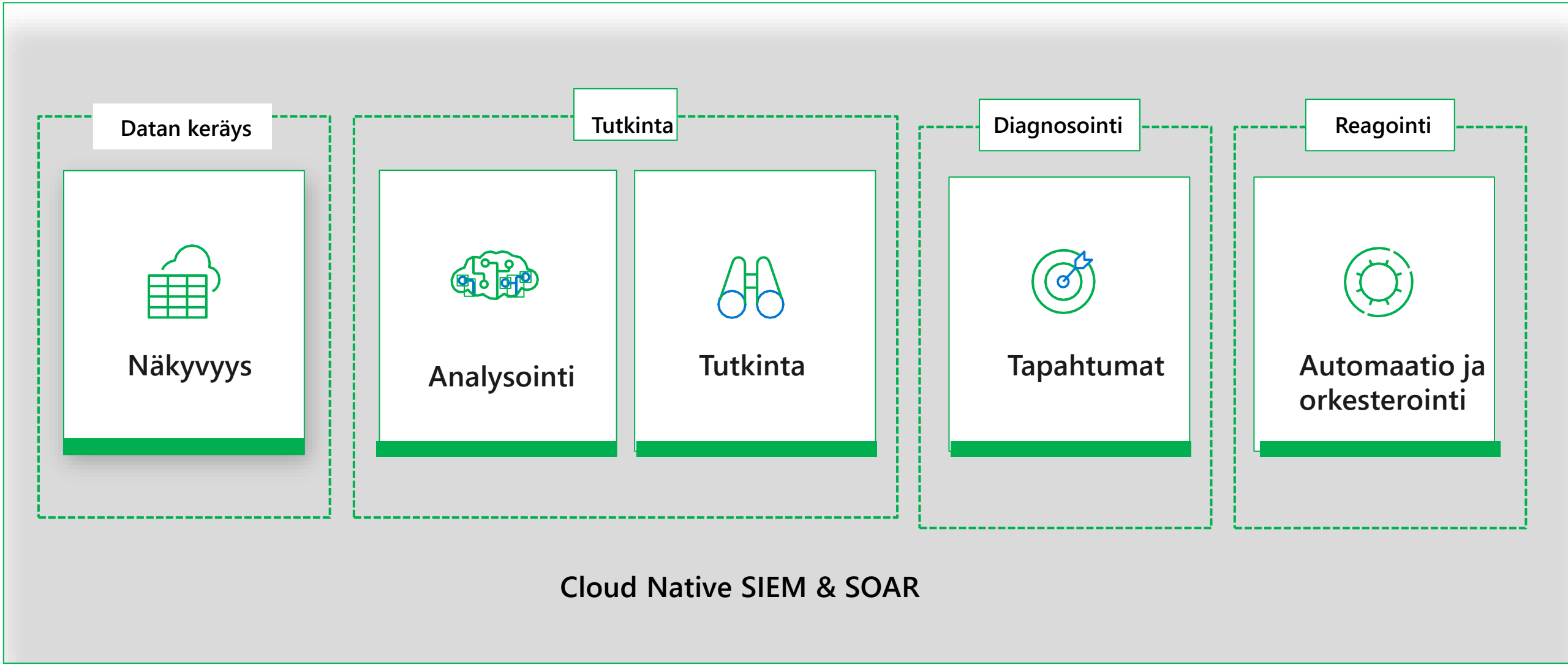
Käyttöönotto nopea ja käyttö joustavaa valmiiden tietoturvan analysointinäkymien myötä sekä käytössä valmiita automaatiomalleja jatkotoimenpiteille.

Moderni ja muokattavissa oleva

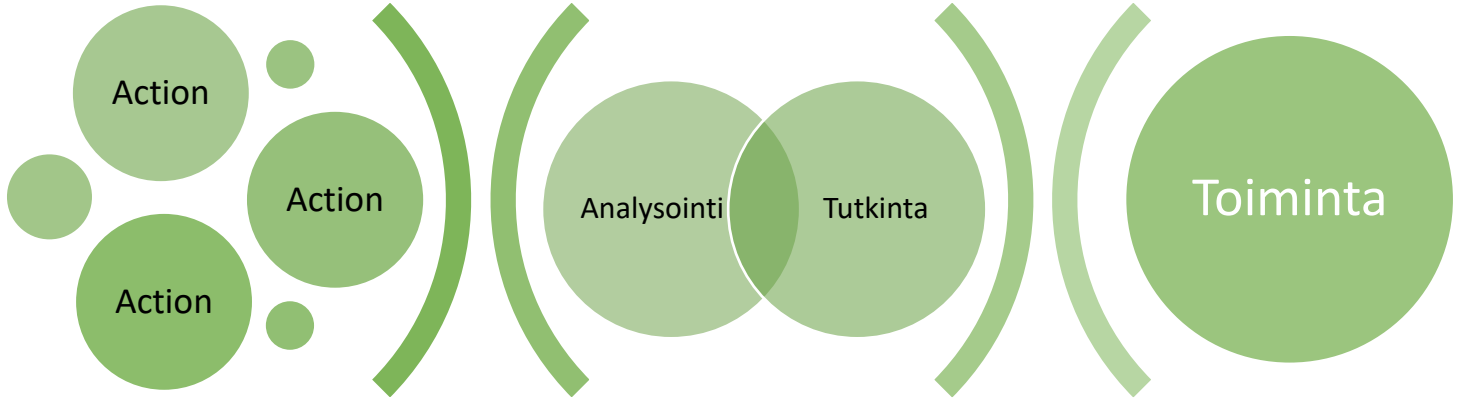
Pilvipohjainen logien hallinta jossa rajapinnat useisiin kolmannen osapuolen järejstelmiin (kuten tietokannat, palomuurit, verkkolaitteet), sisältäen myös valmiin koneoppimis- ja analytiikkasäännöstön.



Kattava tietoturvakokonaisuus



Esimerkki automaatiosta



Kiinniotto:

Ohjataan tapahtuma analysoitavaksi

Tukipyyntö (ServiceNow)

Tapahtumaketjun seuranta

Teams/Slack/tms kanavalla

Laajuus ja vaikuttavuus:

Tarkastetaan IP-osoitteen alkuperä

Käynnistetään Cloud Security – tutkinta

Lähetetään käyttäjälle varmistusviesti

Mitigointi:

Estetään IP-osoite

Estetään käyttäjän pääsy

Aktivoidaan ehdollinen pääsynhallinta

Eristetään kone

Atea **Sentinel Pilotti -projektimalli**

- Workshop 1 – Sentinel –ratkaisun läpikäynti, lokilähteiden kartoitus ja esivaatimukset
- Workshop 2 - Sentinel käyttöönotto; perehdytys, rajapintojen konfigurointi, dashboardit ja analysoinnin käynnistäminen – kahden viikon tiedonkeruujakso
- Workshop 3 - Analysointi ja tilannekuvan tarkastus, kahden viikon tiedonkeruujakso
- Workshop 4 – loppuraportti ja jatkokehitystoimenpiteet

Pilotoinnin **scope**

- Sisältää valmiiden rajapintojen käytön (ei KQL- räätälöityjä)
- Ei sisällä incidenttien ratkaisua (erillisveloitteinen)
- Asiakas vastaa Azure -tilauksesta ja kuluista
- Asiakas vastaa mahdollisista asennuksista omassa ympäristössään liittyen rajapintoihin (neuvonta tuntiveloitteista)
- Mikäli Sentinel halutaan kytkeä mahdollisen kolmannen osapuolen SOC-palveluun, konsultointi laskutetaan tuntiveloitteisesti
- Ei sisällä mahdollisten E5 Security tuotteiden konfigurointeja (Atea M365 Tietoturvapilotti)

We build **Finland** with IT

ATEA