

A photograph of a server room with two men standing in the center, looking at a server rack. The room is filled with rows of server racks, each with many blue indicator lights. The men are dressed in business casual attire. The overall lighting is dim, with the primary light source being the server lights.

# Atea Sentinel Pilotti ja kehitys

Microsoft Sentinel SIEM -  
ratkaisu

---

Etu sukunimi

[Etu.suku@atea.fi](mailto:Etu.suku@atea.fi)

ATEA

# Keskitetyn logien hallinnan hyödyt



## Helppo ja suoraviivainen

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



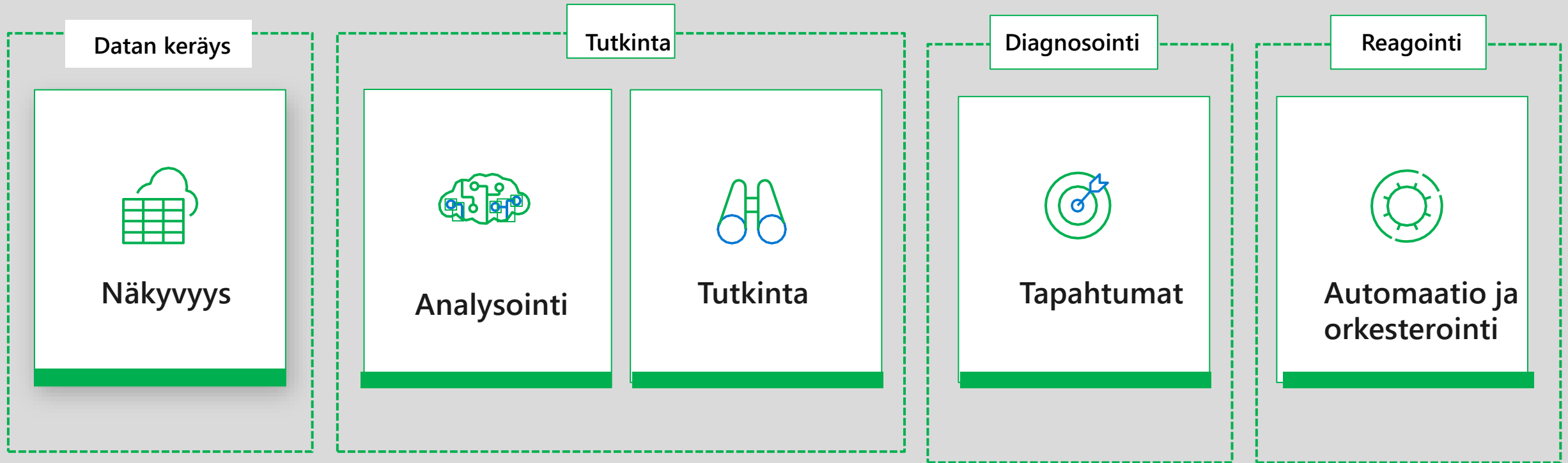
## Moderni ja muokattavissa oleva

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

The screenshot displays the Microsoft Sentinel 'Active rules' page. At the top, there are 51 active rules, categorized by severity: 12 High, 26 Medium, 9 Low, and 4 Informational. A table lists various rules, including 'Known Phosphorus group domains', 'Advanced Multistage Attack...', and 'Create incidents based on Azure Acti...'. The 'Known Phosphorus group domains' rule is selected, showing its details on the right. The rule is a 'Scheduled' type, requiring 'DNS (Pr... +2)' data sources and using 'Command and Control' tactics. The rule query is shown as:

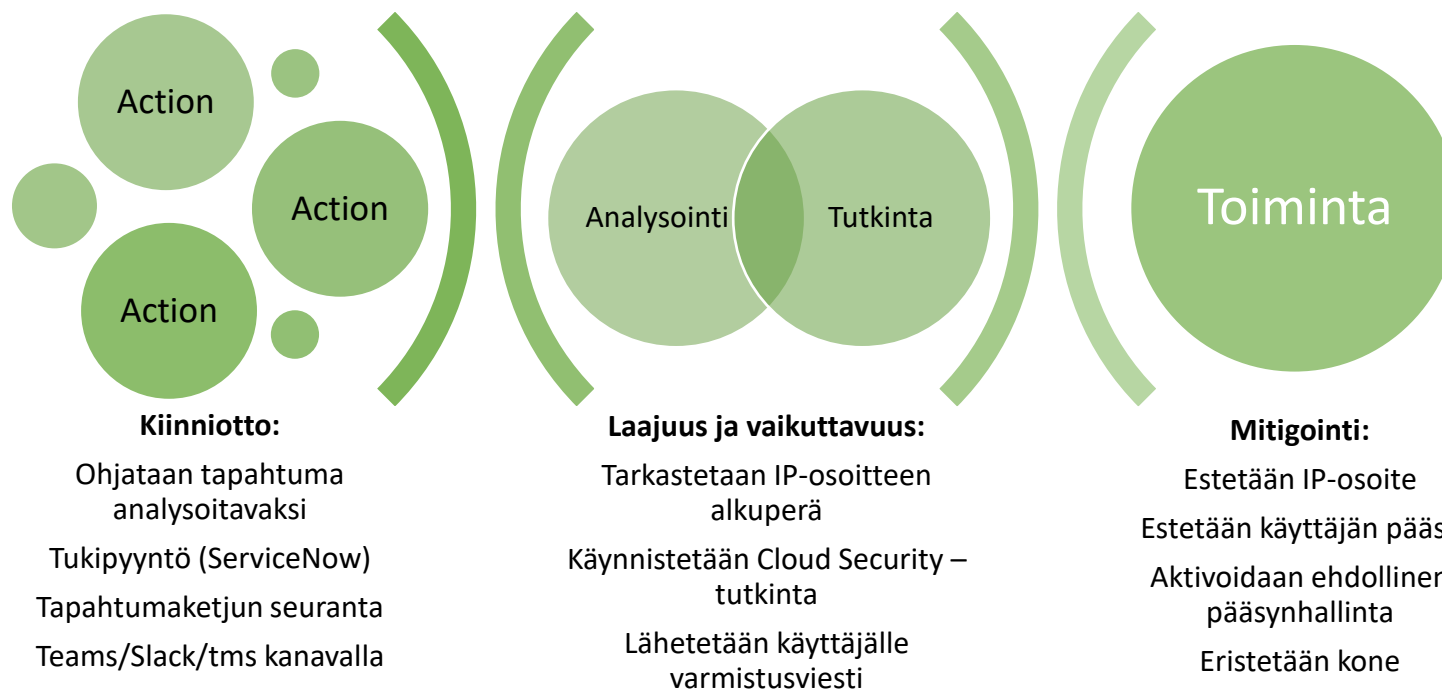
```
let timeframe = 1d;
let DomainNames = dynamic(["yahoo-verification.org", "s
"accounts-web-mail.com", "customer-certificate.com", "se
"yahoo-verification.net", "yahoo-verify.net", "outlook-v
```

# Kattava tietoturvakokonaisuus



Cloud Native SIEM & SOAR

# Esimerkki automaatiosta





# 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)



ATEA

We build **Finland** with IT

ATEA