Pilven AI-sovellukset ja infra – Miten ne suojataan ja miksi suojaaminen on tärkeää?

Arrow x Microsoft Kumppaniarkkitehtiseminaari 12.6.2024

aka.ms/kumppaniarkkitehtiseminaari

HAHMOT STAGELLA

Markus Lintuala
Elisa Oyj

Timo Salminen
Microsoft Oy

Mitä on organisaatiosi prioriteettilistalla?

⚠	**Ransomware palautumiskyky**	*Aloituspvm / Käynnissä*
#	**Pääsynhallinta ja -suojaus**	*Aloituspvm / Käynnissä*
#	**Modernit tietoturvaratkaisut**	*Aloituspvm / Käynnissä*
#	**Infrastruktuuri ja kehitys**	*Aloituspvm / Käynnissä*
#	**Datan suojaus ja riskienhallinta**	*Aloituspvm / Käynnissä*
#	**OT ja IoT Tietoturva**	*Aloituspvm / Käynnissä*
#	**Julkinen uhkapinta-ala**	*Aloituspvm / Käynnissä*

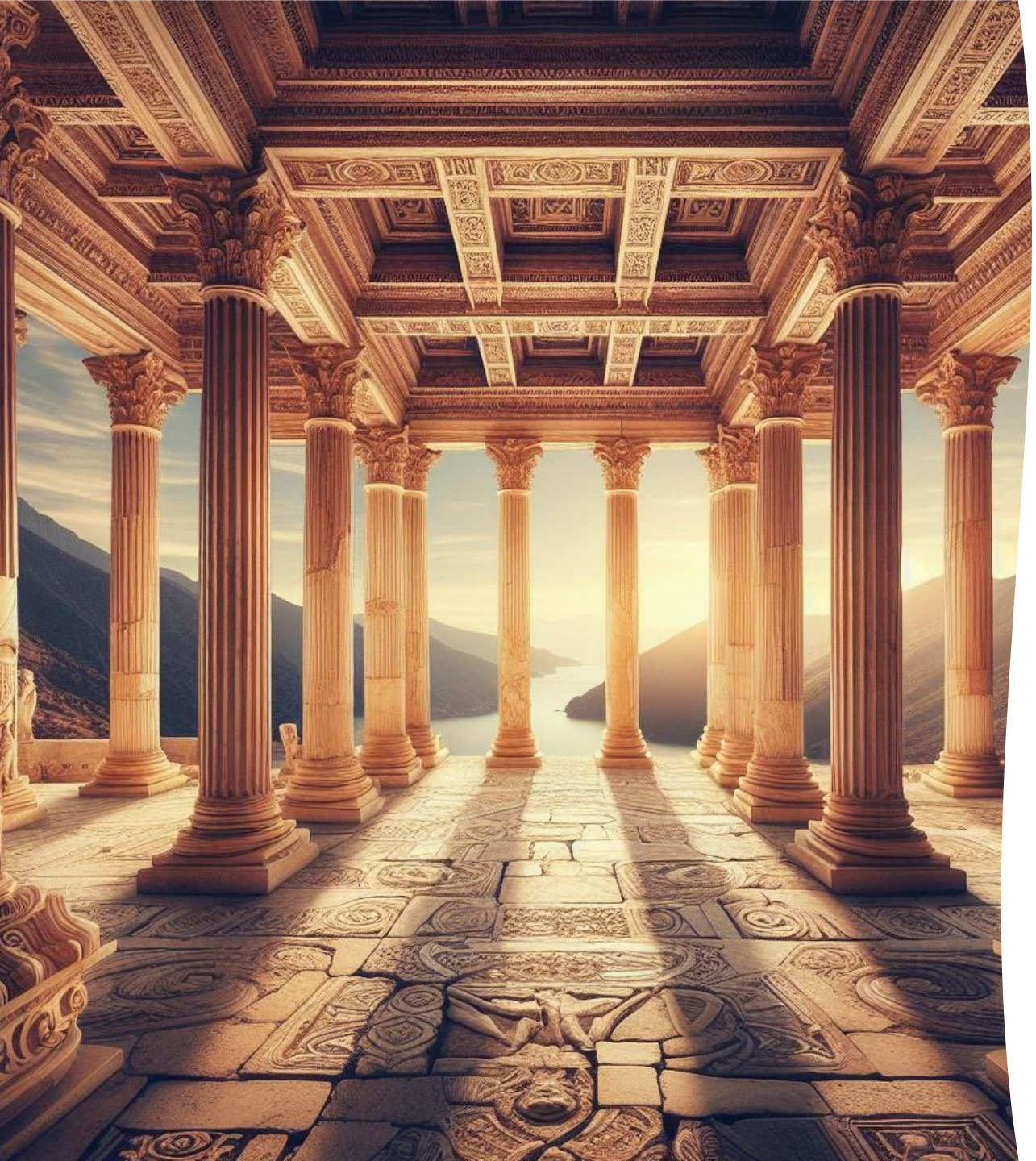
Azure-ympäristö

DEMO

Asiakasympäristöstä löydettyä

Yhteenveto löydöksistä

- Verkkokauppa asunut joskus virtuaalitietokoneissa
- Uudistettu Azuren natiiviksi toteutukseksi kontissa
- Seminaarista ostettu OpenAI-pohjainen ChatBot joka halutaan kauppaan palvelemaan asiakkaita
- Näkee, että hallintamalli on hakusessa ja ympäristö ei ole parhaiden käytäntöjen mukaisesti rakennettu



Julkipilven peruspilarit

- Hallintamalli paikallaan, ei vain kansiossa hyllyn päällä
- Tietoturva ulotettu eri ratkaisuihin
- Arkkitehtuuri suunniteltu läpi julkaisuketjun
- Kustannustehokkuus

Nykytilan analysointi

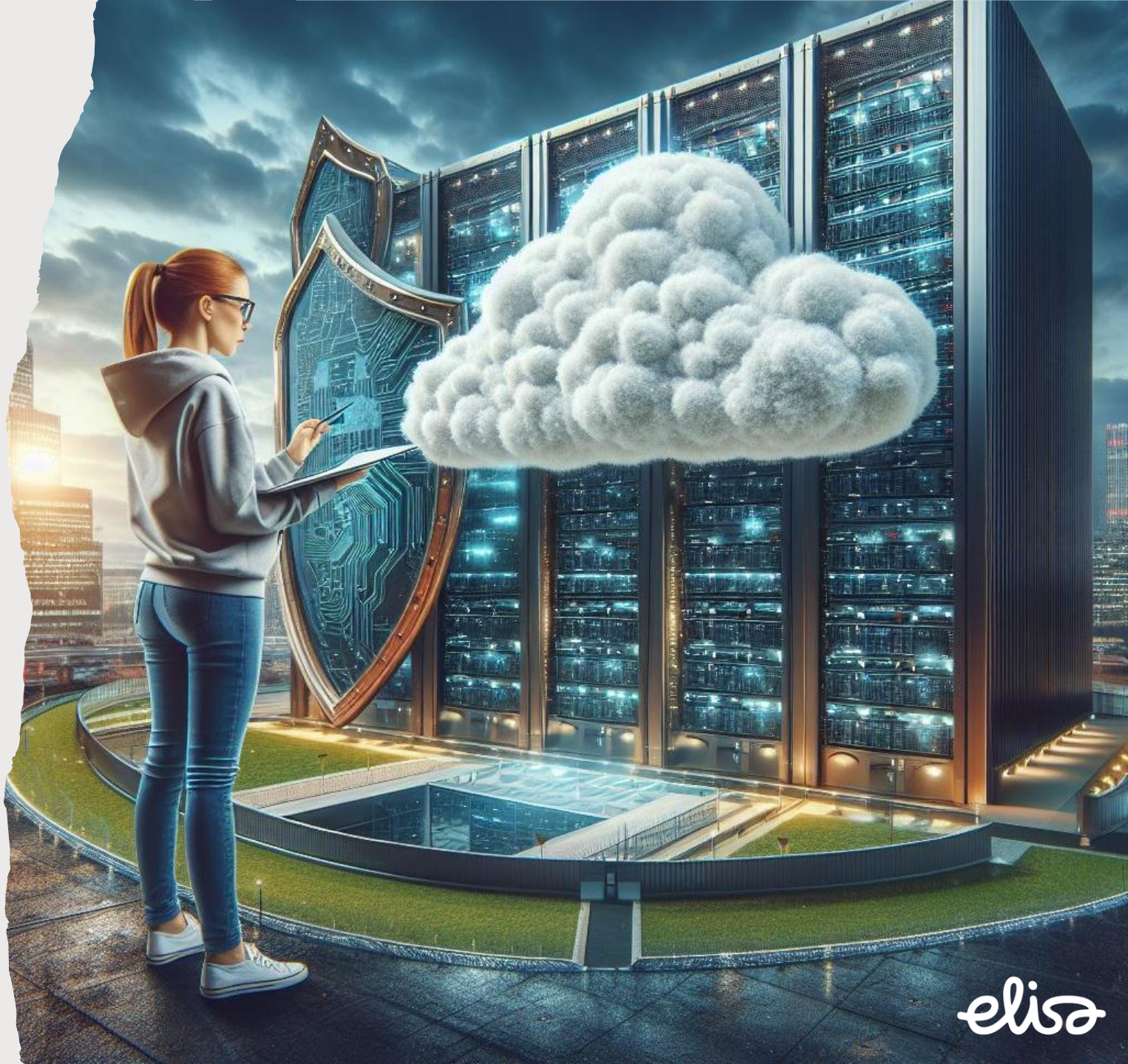
- Arkkitehtuurin katselmointi
- Konfiguraatiot ja cloud security posture management
- Julkinen ja sisäinen uhkapinta-ala
- Julkaistujen sovellusten liikenteen valvonta
- Logitukset ja monitorointi

DEMO

Defender for Cloud
CSPM

Julkisen uhkapinta-alan valvonta

- Tunnista julkaistujen sovellusten avoimia portteja, haavoittuvuuksia sekä ulkoapäin tunnistettavia konfiguraatiovirheitä
- Määritä itse, mitä skannataan ja mitä valvotaan
- Keskitä havainnot Sentineliin



DEMO

External Attack Surface Management

SHODAN

// FOUND **751,708** RE

172.160.225.163

Microsoft Limited

Sweden, Gävle

cloud self-signed

SSL Certificate

Issued By:

|- Common Name:

verkkokauppa-wi

Issued To:

|- Common Name:

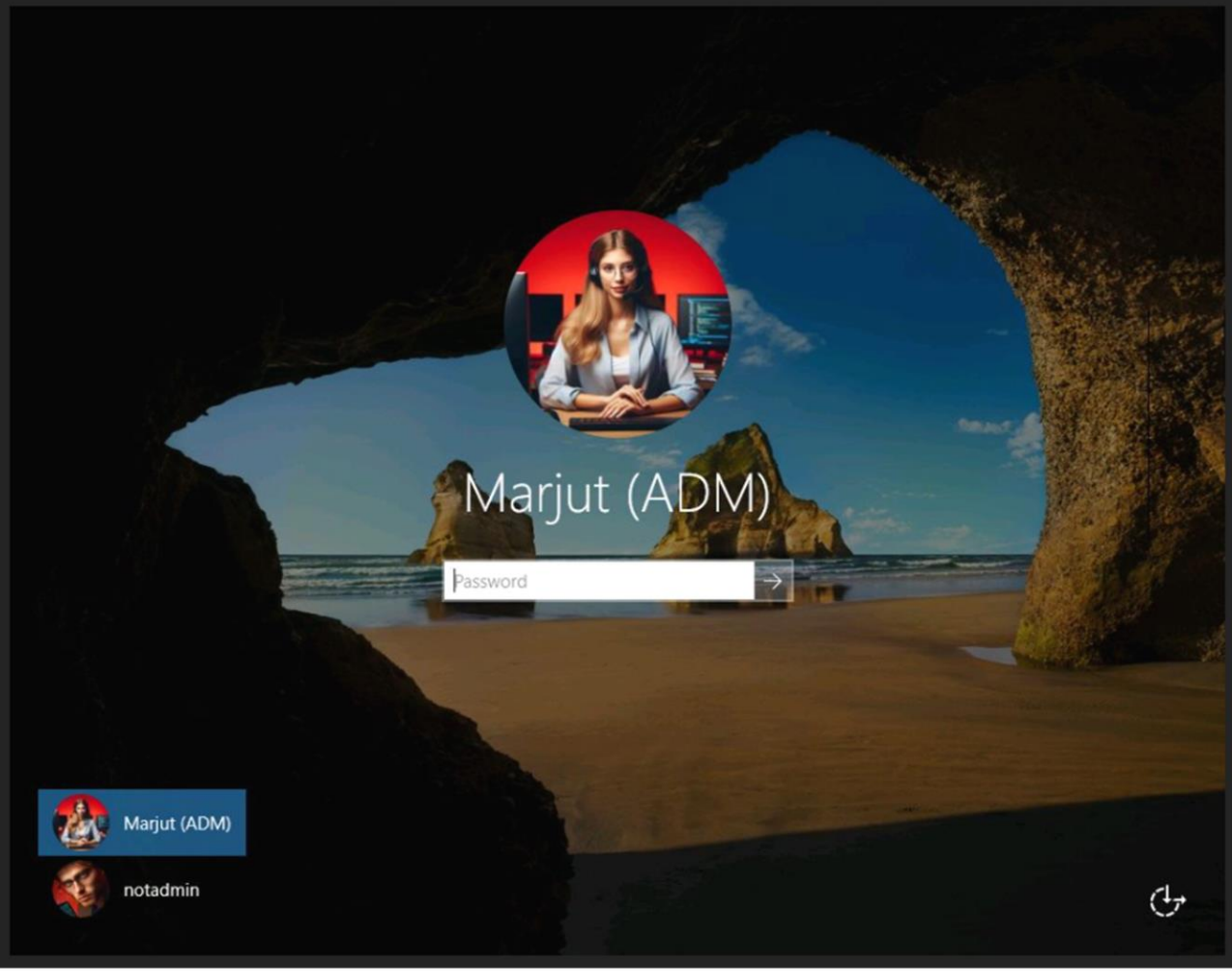
verkkokauppa-wi

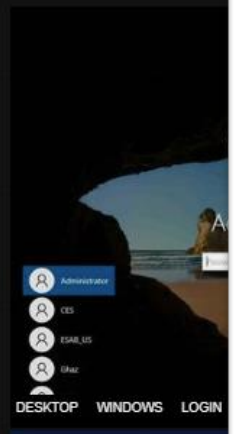
Supported SSL Versions:

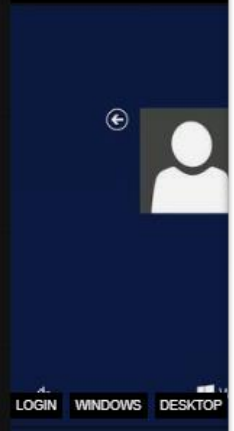
TLSv1, TLSv1.1, TLSv1.2

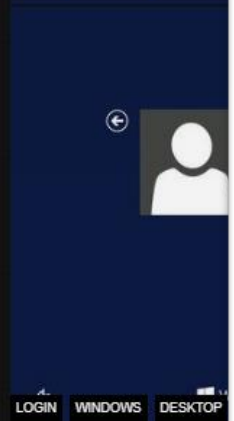
2024-04-11T05:44:32.761072

```
Remote Desktop Protocol
\x03\x00\x00\x13\x0e\xd0\x00\x00\x124\x00\x02\x1f\x08\x00\x02\x00\x00\x00
Remote Desktop Protocol NTLM Info:
  OS: Windows 10 (version 1607)/Windows Server 2016 (version 1607)
  OS Build: 10.0.14393
  Target Name: verkkokauppa-wi
  NetBIOS Domain Name: verkkokauppa-wi
  Ne...
```







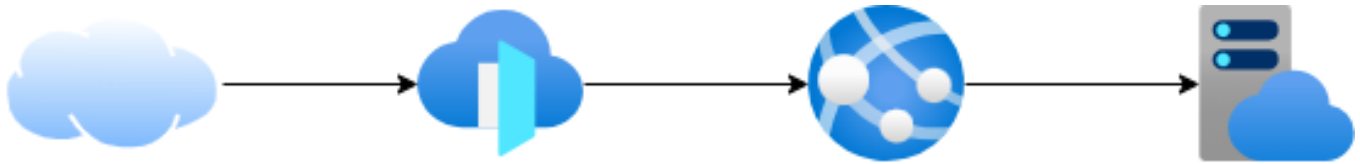


Sovellusten julkaisun suojaaminen

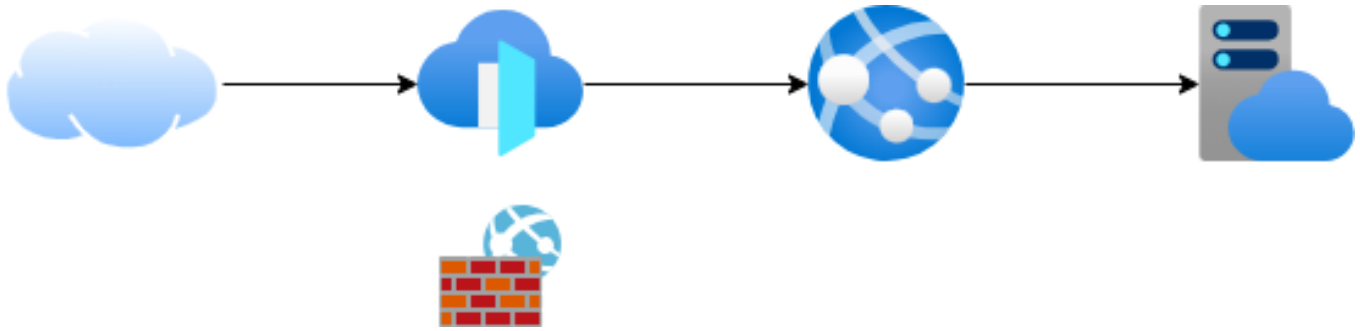
- Ota käyttöön keskitetty Front Door tai Application Gateway
- Rajapintojen julkaisu Azure API Managementin avulla
- Käytä web application firewallia sovelluksiesi lisäsuojana

DEMO

WAF ja nettikauppa



Demo: WAF ja nettikauppa



Demo: WAF ja nettikauppa

Mitä tekee WAF?

- Web Application Firewall
- Lisäpalvelu, joka toimii Layer7 tasolla ja tutkii jokaisen HTTP-pyynnön
- HTTP-liikenteessä voi olla mukana murtautujien ponnisteluja löytää webbipalvelusta heikkouksia
- WAF tunnistaa nämä ponnistelut ja joko lokittaa ne tarkempaa tutkimusta varten tai suoraan estää pyynnön, jos havaitsee sen sääntöjen vastaiseksi
- WAF skaalautuu automaattisesti liikenteen kuorman mukaan

403 Forbidden

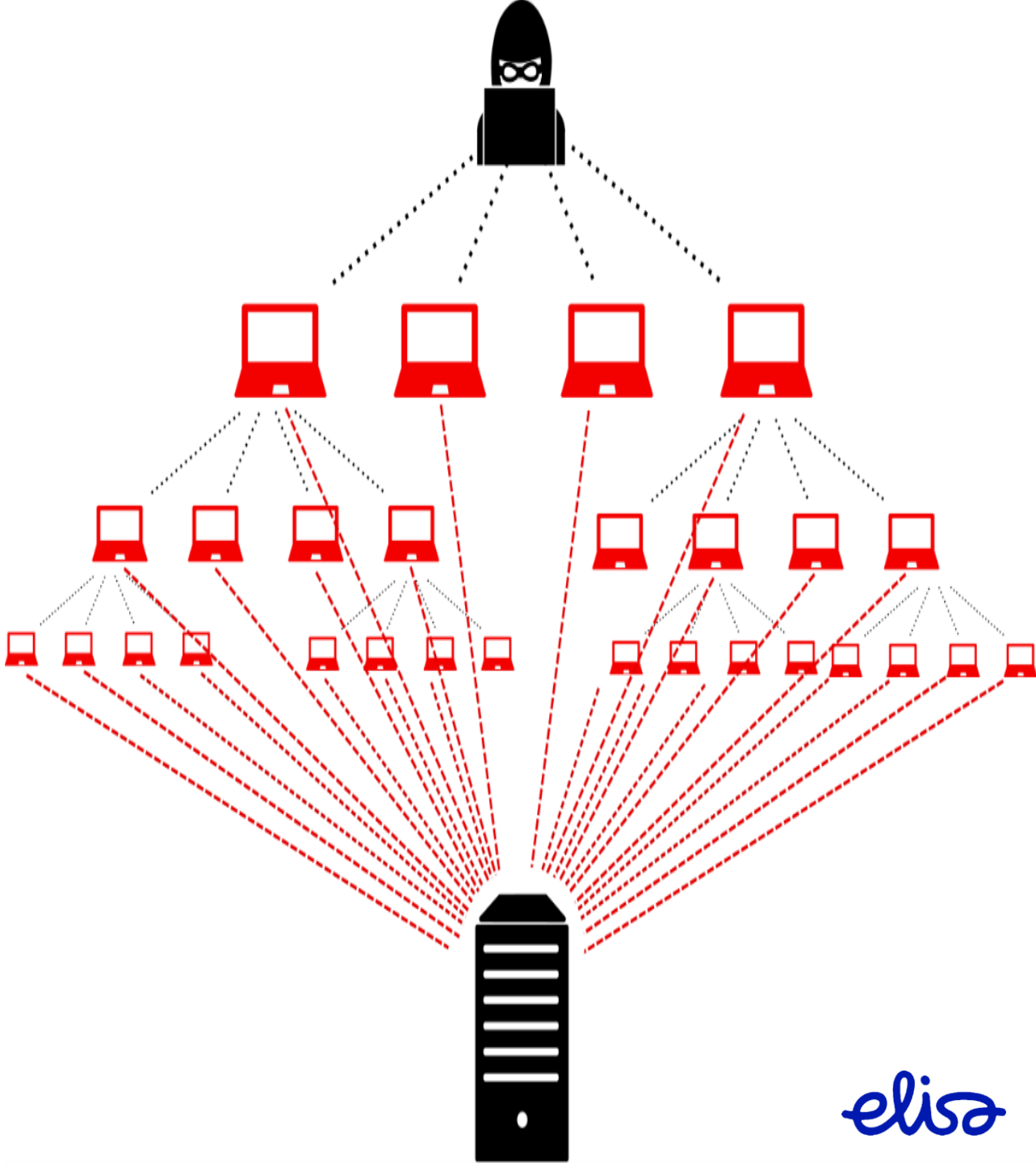
Microsoft-Azure-Application-Gateway/v2

WAF parhaat käytänteet

- Julkaistavat sovellukset ja niiden toiminnallisuudet syytä tuntea, linkki kehittäjiin ei haittaa lainkaan vianselvitystä
- Multisite – arkkitehtuurissa sijoita globaaliin sääntöön mahdollisimman vähän rajoituksia, tee rajoitukset sovelluskohtaisesti
- WAF Triage workbook näyttää lokien tiedot mukavasti ja sen avulla pystyt päättelemään, mikä sääntö on liian tiukalla
- Aloita omien sääntöjen laatiminen helpoista, esim. "älä salli mitään liikennettä Pohjois-Koreasta"

DDOS hyökkäys

- Yleensä varsin lyhytkestoisia, mutta massiivisia
- Hyökkääjä jää usein tunnistamatta, koska he käyttävät zombie-koneita varsinaiseen hyökkäykseen (zombie voi olla kotikoneesi)
- Hyökkäykset ajoitetaan usein silloin, kun niille saadaan paras vaikuttavuus



Mitä tekee DDOS protection?

- DDOS protection tutkii kaikkea IP-osoitteelle tulevaa liikennettä. Tutkimisessa hyödynnetään kehittyneitä tekoälypohjaisia menetelmiä
- Mikäli liikenteessä havaitaan palvelunestohyökkäyksen tunnusmerkkejä, liikenne suodatetaan pois
- Palvelu voidaan ottaa käyttöön suojaan yhtä IP-osoitetta (per ip) tai useampaa (DDOS standard)
- DDOS standardiin sisältyy Microsoftin takuu palvelun häiriöttömyydelle verkkohyökkäyksen aikana sekä DDoS Rapid Response – palvelun, josta saa tarvittaessa apua hyökkäyksen torjumisessa

Defender for Cloud tehokäyttöön

- Ainut tapa suojata Azuren PaaS-infrastruktuurin komponentteja ja lisätä näkyvyyttä konepellin alle
- Keskitä infrastruktuurin tietoturvanäkymä yhteen paikkaan riippumatta sen sijainnista – Azure Arc
- Yhdistä DevOps-tuotteesi samaan työkaluun keskitetyn näkymän saamiseksi
- Valjasta kehittäjät saamaan sovelluksista automaattiset herätteet, mikäli huomautettavaa on

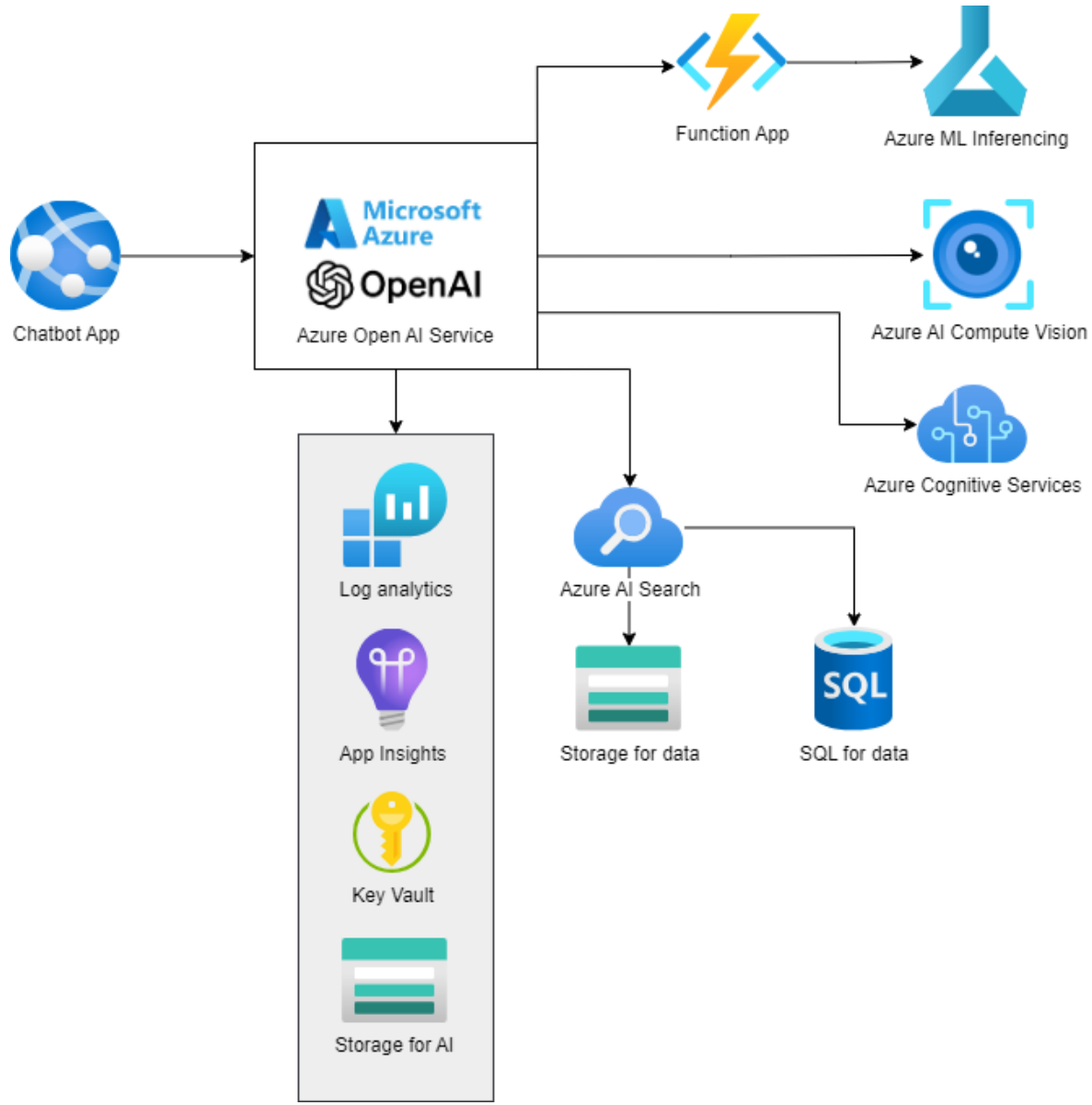
DEMO

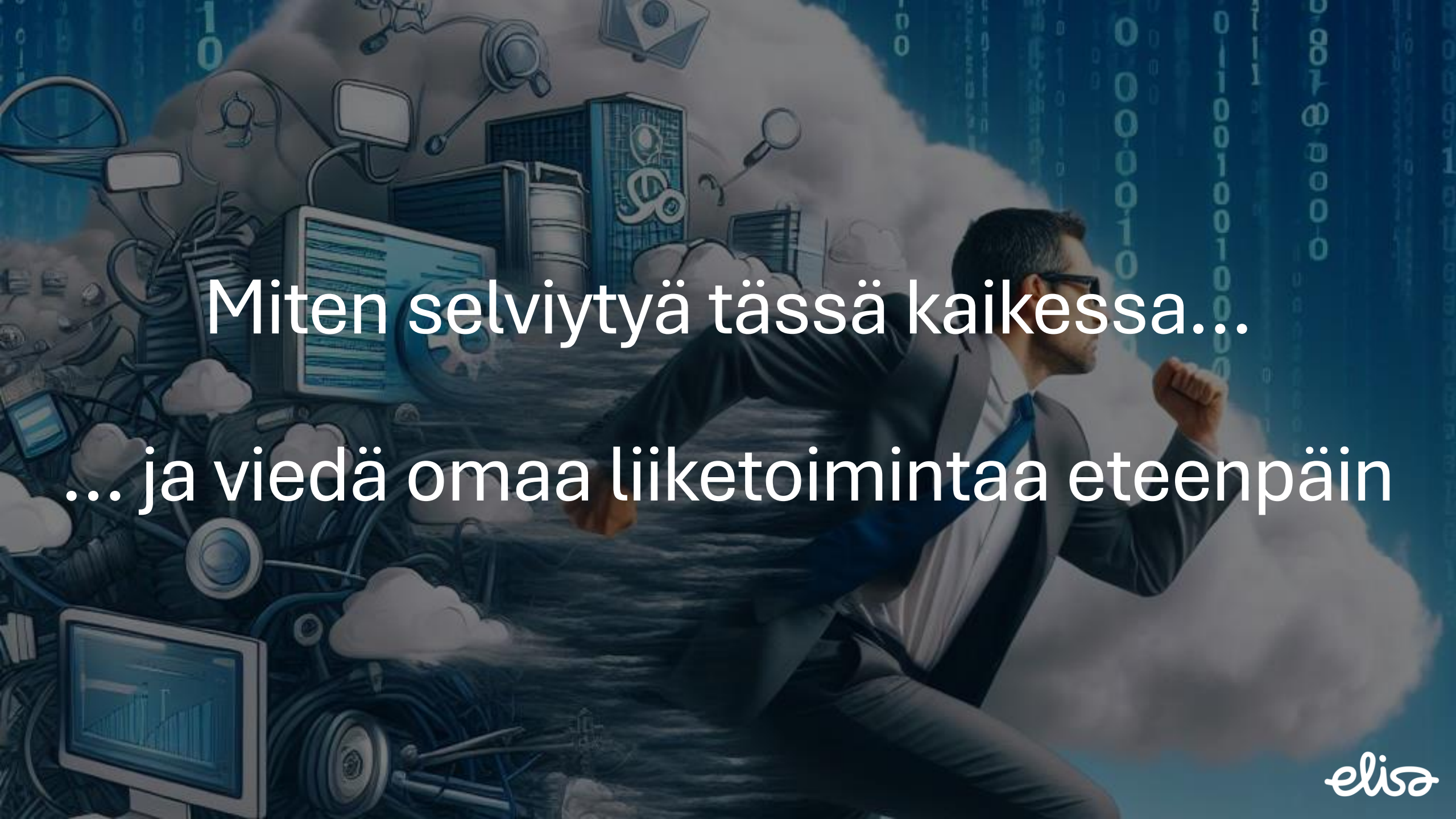
Defender for Cloud

Azure Open AI Services

- Sovellusrajapinta isoihin kielimalleihin
- Tuote kuten mikä tahansa muu pilviratkaisu
- Suojaa pääsy, suosi managed identityä
- Muista suojata yhtälailla mahdollinen vektorikanta ja muut ulkoiset toiminteet
- Huomioi pääsynhallinta datan osalta

Azure OpenAI Services arkkitehtuuri




Miten selviytyä tässä kaikessa...
... ja viedä omaa liiketoimintaa eteenpäin

Kolme pointtia kotiin

- Hanki näkyvyys sisältä ja ulkoa sekä käytä pilven skaalautuvia tietoturvaratkaisuja
- Käsittele tekoälyn resursseja kuin mitä tahansa muuta pilven resurssia
- Aja kovaa – järki päässä

Kiitos!

Esitykset ja tallenteet ovat ladattavissa osoitteessa:
https://aka.ms/kumppaniarkkitehtiseminaari