MOSADEX E-HEALTH

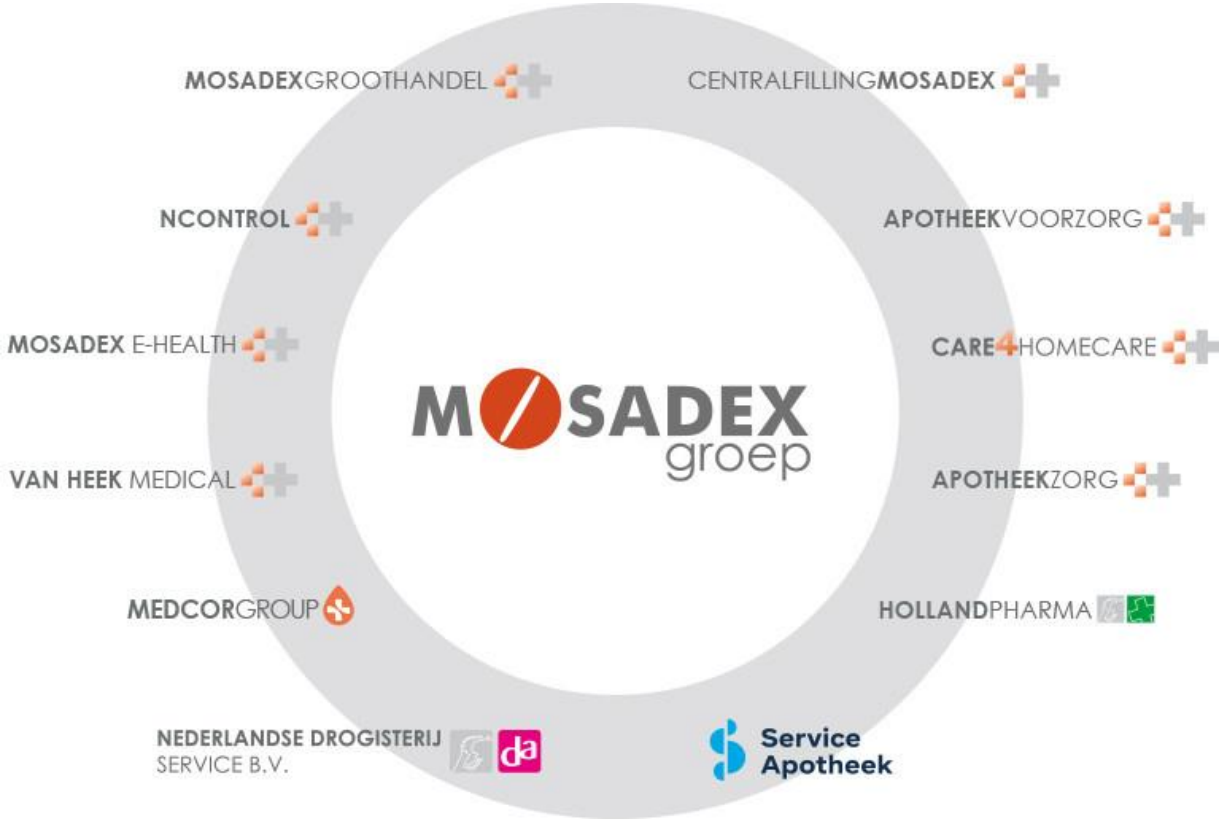
Onderdeel van Mosadex Groep

Joost Koppers

Unit Manager

Cloud, Data & Security

Wij ontwikkelen software **voor een** betere zorg



MOSADEX E-HEALTH
Onderdeel van Mosadex Groep

Grip op Cloud Security

Effectief gebruik van de Secure Score in Defender for Cloud

DUTCH MICROSOFT SECURITY MEETUP

Even voorstellen…

Charlotte Leuverink

Cloud Security Engineer

MOSADEX E-HEALTH

Onderdeel van Mosadex Groep

Het Cloud & Security team

Ondersteunen van developers & ‘verservicen’ van onze Cloud omgeving

Cloud & Security team

- Cloud (Security) engineers
- Expertise: Azure/Terraform

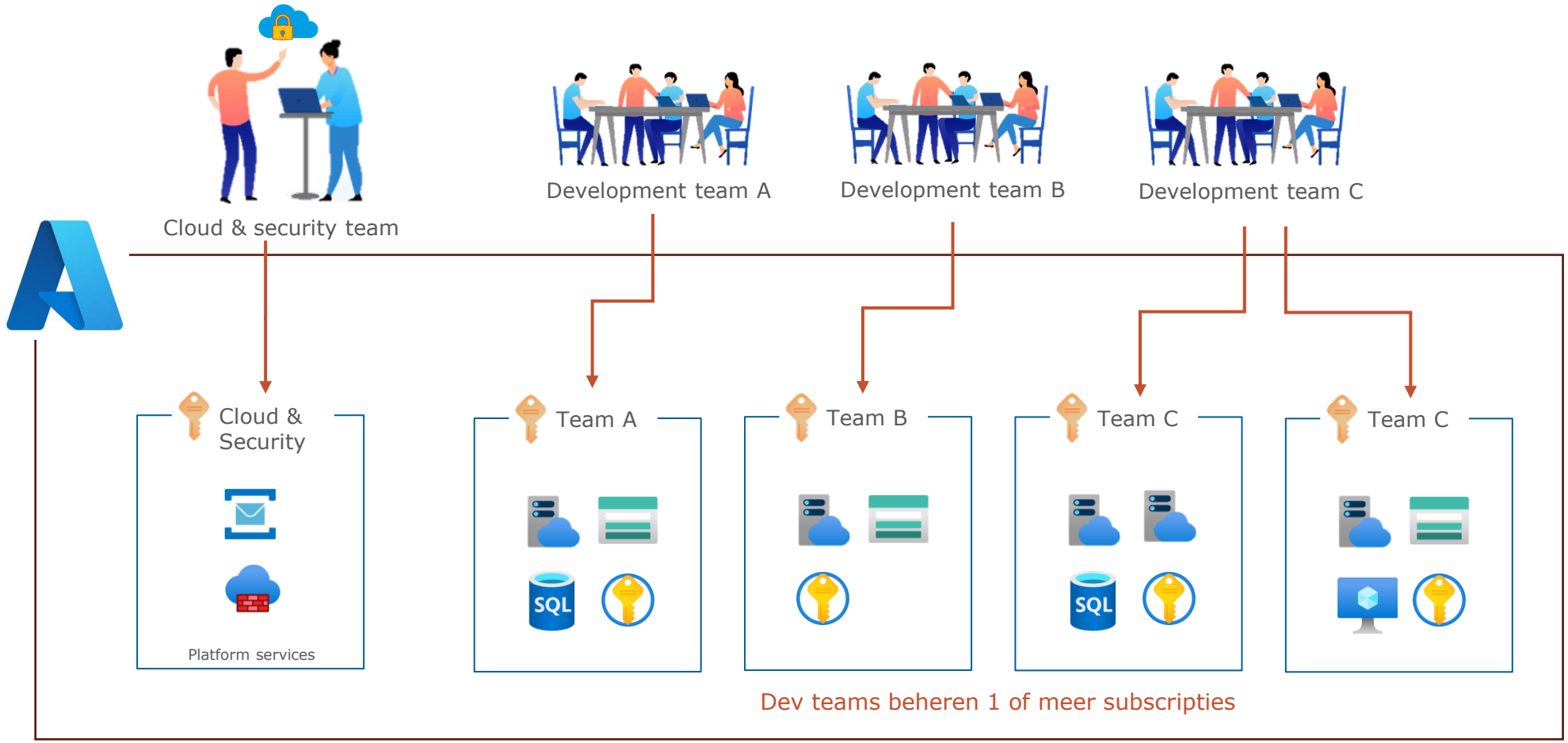
Ondersteunt

Development teams

- Software developers
- Expertise: C#/.NET

Autonome development teams

Elk team is verantwoordelijk voor hun eigen Azure resources



Elk team is verantwoordelijk voor eigen Azure resources

Elk team is verantwoordelijk voor
de security van eigen Azure resources

Het Cloud & Security team

Ondersteunen van developers & ‘verservicen’ van onze Cloud omgeving

Cloud & Security team

- Cloud (Security) engineers
- Expertise: Azure/Terraform

Ondersteunt

Development teams

- Software developers
- Expertise: C#/.NET

Er zijn **zo veel** opties

Hoe weet je welke opties je kiest?

Ik ben een developer en ik wil **een file opslaan.**

Hoe weet je welke opties je kiest?

Ik ben een developer en ik wil **een file opslaan.**

Dus ik moet een **storage account** **uitrollen.**

Create a storage account

Security

Configure security settings that impact your storage account.

- Require secure transfer for REST API operations ⓘ — [x]
- Allow enabling anonymous access on individual containers ⓘ — [ ]
- Enable storage account key access ⓘ — [x]
- Default to Microsoft Entra authorization in the Azure portal ⓘ — [ ]
- Minimum TLS version ⓘ — Version 1.2
- Permitted scope for copy operations (preview) ⓘ — From any storage account

Hierarchical Namespace

Hierarchical namespace, complemented by Data Lake Storage Gen2 endpoint, enables file and directory semantics, accelerates big data analytics workloads, and enables access control lists (ACLs) Learn more

- Enable hierarchical namespace ⓘ — [ ]

Access protocols

Blob and Data Lake Gen2 endpoints are provisioned by default Learn more

- Enable SFTP ⓘ — [ ]
  - ⓘ SFTP can only be enabled for hierarchical namespace accounts
- Enable network file system v3 ⓘ — [ ]
  - ⓘ To enable NFS v3 'hierarchical namespace' must be enabled. Learn more about NFS v3

Blob storage

- Allow cross-tenant replication ⓘ — [ ]
- Access tier ⓘ — (•) **Hot:** Optimized for frequently accessed data and everyday usage scenarios

Create a storage account

Network connectivity

You can connect to your storage account either publicly, via public IP addresses or service endpoints, or privately, using a private endpoint.

Network access *

- (•) Enable public access from all networks
- ( ) Enable public access from selected virtual networks and IP addresses
- ( ) Disable public access and use private access

Enabling public access from all networks might make this resource available publicly. Unless public access is required, we recommend using a more restricted access type. Learn more

Network routing

Determine how to route your traffic as it travels from the source to its Azure endpoint. Microsoft network routing is recommended for most customers.

Routing preference * ⓘ

- (•) Microsoft network routing
- ( ) Internet routing

Create a storage account

Recovery

Protect your data from accidental or erroneous deletion or modification.

- [ ] Enable point-in-time restore for containers
  Use point-in-time restore to restore one or more containers to an earlier state. If point-in-time restore is enabled, then versioning, change feed, and blob soft delete must also be enabled. Learn more

- [x] Enable soft delete for blobs
  Soft delete enables you to recover blobs that were previously marked for deletion, including blobs that were overwritten. Learn more
  Days to retain deleted blobs: 7

- [x] Enable soft delete for containers
  Soft delete enables you to recover containers that were previously marked for deletion. Learn more
  Days to retain deleted containers: 7

- [x] Enable soft delete for file shares
  Soft delete enables you to recover file shares that were previously marked for deletion. Learn more
  Days to retain deleted file shares: 7

Tracking

Manage versions and keep track of changes made to your blob data.

- [ ] Enable versioning for blobs
  Use versioning to automatically maintain previous versions of your blobs. Learn more

  Consider your workloads, their impact on the number of versions created, and the resulting costs. Optimize costs by automatically managing the data lifecycle. Learn more

- [ ] Enable blob change feed
  Keep track of create, modification, and delete changes to blobs in your account. Learn more

Access control

- [ ] Enable version-level immutability support
  Allows you to set time-based retention policy on the account-level that will apply to all blob versions. Enable this feature to set a

Create a storage account

Encryption type * ⓘ
- (•) Microsoft-managed keys (MMK)
- ( ) Customer-managed keys (CMK)

Enable support for customer-managed keys ⓘ
- (•) Blobs and files only
- ( ) All service types (blobs, files, tables, and queues)

⚠ This option cannot be changed after this storage account is created.

Enable infrastructure encryption ⓘ [ ]

EXAMS

Exam SC-100: Microsoft Cybersecurity Architect

As a Microsoft cybersecurity architect, you translate a cybersecurity strategy into capabilities that protect the assets, business, and operations of an organization. You design, guide the implementation of, and maintain security solutions that follow Zero Trust principles and best practices, including security strategies for:

- Identity
- Devices
- Data
- Applications
- Network
- Infrastructure
- DevOps

Hoe weet je welke opties je kiest?

Ik ben een developer en ik wil **een file opslaan.**

Dus ik moet een **storage account** **uitrollen.**

Maar welke settings moet ik allemaal kiezen?

Hoe houden we grip op cloud security in een organisatie met autonome development teams?

Grip op Cloud Security: drie fases

Vóór deployment:

Terraform Engineering standards

Tijdens deployment:

Azure policies

Na deployment:

Secure Score in Defender for Cloud

Hoe houden we grip op cloud security in een organisatie met autonome development teams?

Vóór deployment:
Terraform Engineering standards

AZURERM DOCUMENTATION

Filter

azurerm provider

- Guides
- AAD B2C
- API Management
- Active Directory Domain Services
- Advisor
- Analysis Services
- App Configuration
- App Service (Web Apps)
- Application Insights
- Arc Resource Bridge
- ArcKubernetes
- Attestation
- Authorization
- Automanage
- Automation

azurerm_key_vault

Manages a Key Vault.

Example Usage

Copy

```
provider "azurerm" {
  features {
    key_vault {
      purge_soft_delete_on_destroy    = true
      recover_soft_deleted_key_vaults = true
    }
  }
}

data "azurerm_client_config" "current" {}

resource "azurerm_resource_group" "example" {
  name     = "example-resources"
  location = "West Europe"
}

resource "azurerm_key_vault" "example" {
  name                        = "examplekeyvault"
  location                    = azurerm_resource_group.example.location
  resource_group_name         = azurerm_resource_group.example.name
```

Terraform Engineering Standards

Infrastructure as Code (IaC) templates voor het uitrollen van Azure Resources

Cloud security engineer

Ontwikkelt

Developer

Gebruikt

Engineering standard

Rolt resource uit met
de juiste config

Terraform Engineering Standards

Infrastructure as Code (IaC) templates voor het uitrollen van Azure Resources

- **Alle config is in code**
  - Overzichtelijk changes bijhouden
  - Alles kan makkelijk opnieuw uitgerold worden
- **Consistente configuraties** over het hele landschap
- We kiezen onze eigen **secure defaults**

Hoe weet je welke opties je kiest?

Ik ben een developer en ik wil **een file opslaan.**

Dus ik moet een **storage account** **uitrollen.**

Ik gebruik de **Engineering Standard** van het Cloud & Security Team!

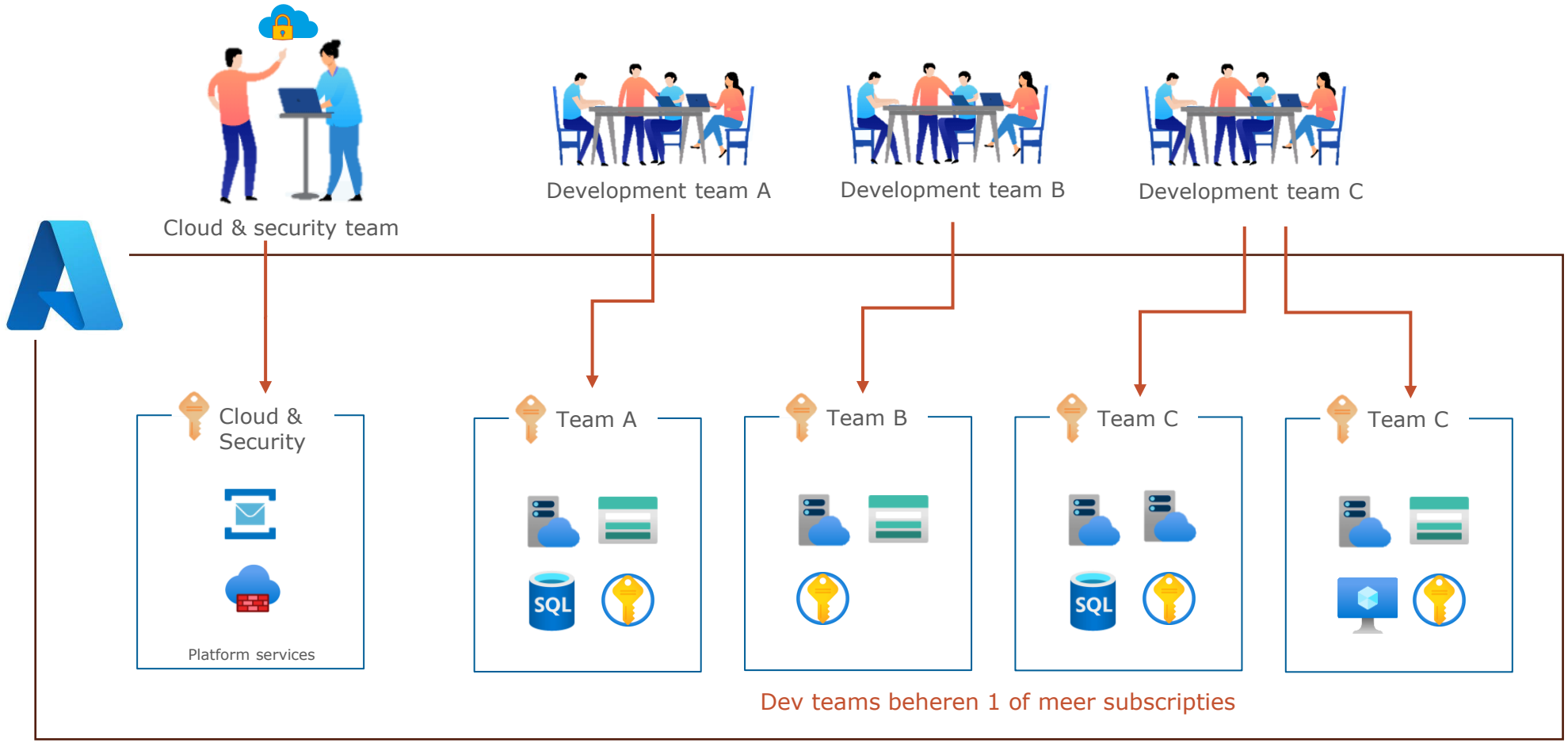
Hoe houden we grip op cloud security in een organisatie met autonome development teams?

Na deployment:
Secure Score in Defender for Cloud

Doel: De secure score moet omhoog

Autonome development teams

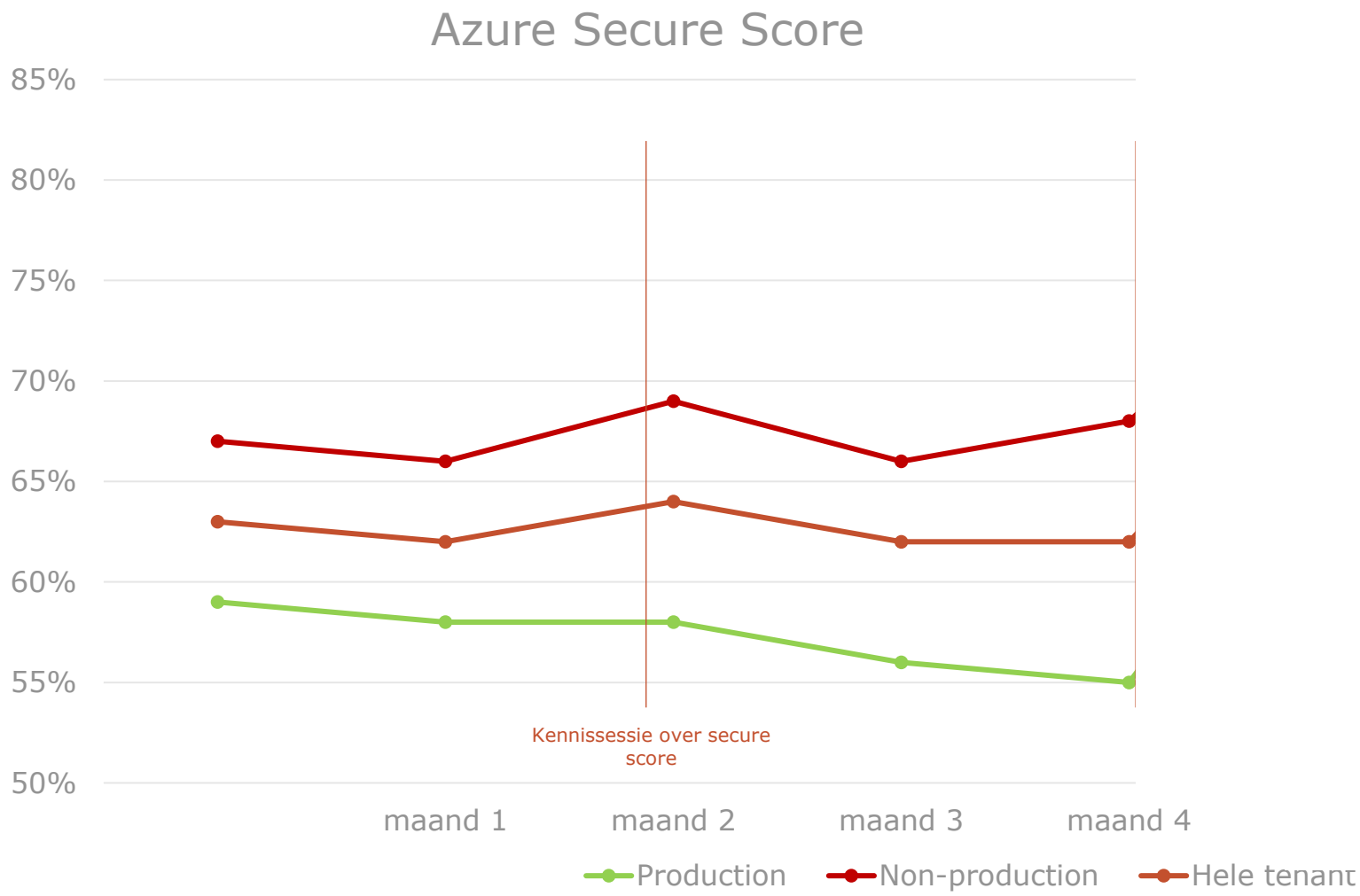
Elk team is verantwoordelijk voor hun eigen Azure resources



De teams moeten zelf aan de slag.

Interne kennissessie over Defender for Cloud

Dit had nog niet veel effect…



Hoe gaan we de teams **motiveren**
om zelf de secure score te verbeteren?

Hoe gaan we de teams **motiveren**
om zelf de secure score te verbeteren?

Maak er een wedstrijdje van!

MOSADEX E-HEALTH

WAR ON COMPLEXITY

HALL OF FAME

* QUARTER-WINNER

QUARTER GREATEST

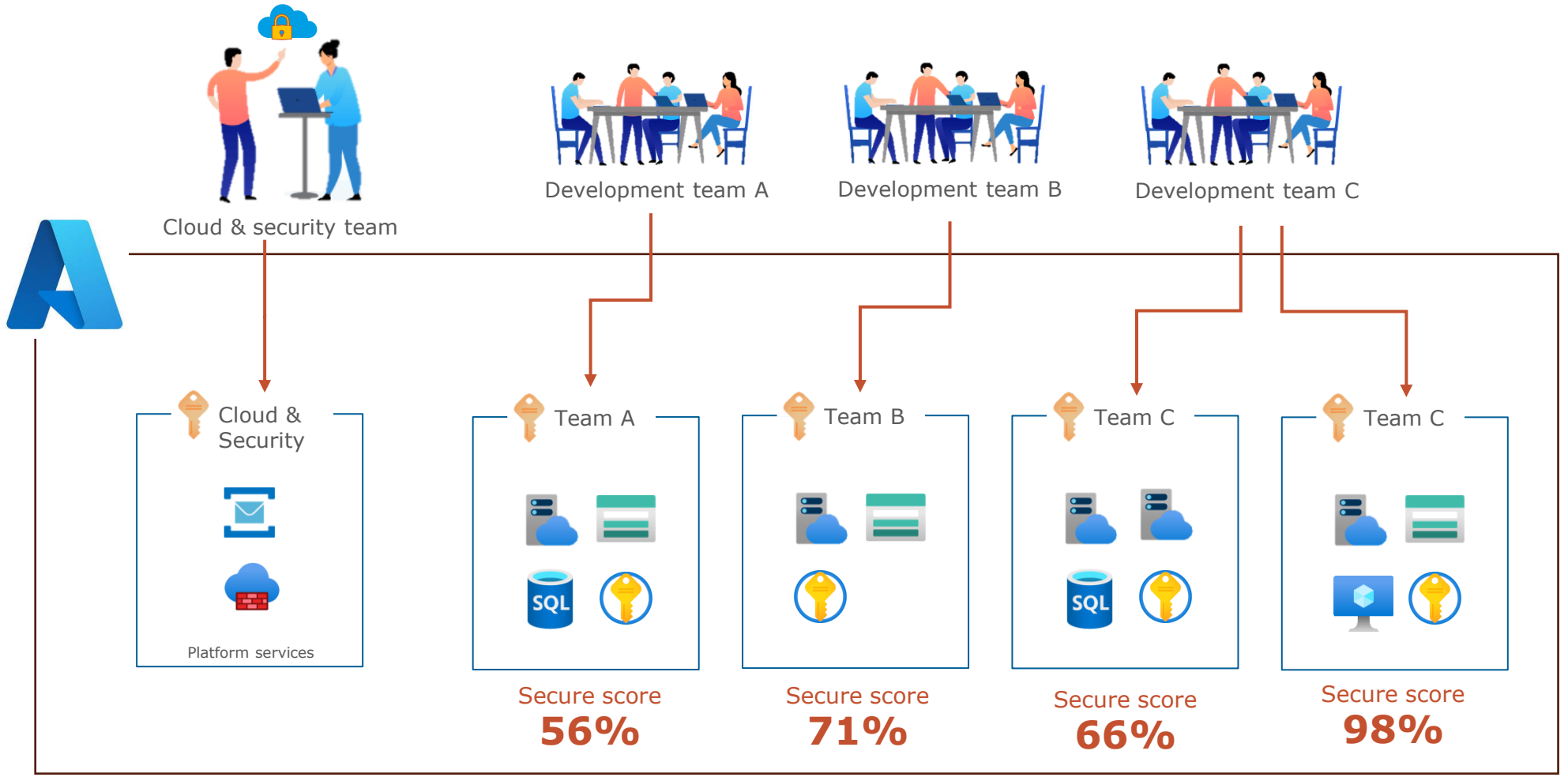
1.	Apollo	0
2.	Cloud	0
3.	Connect	0
4.	Data	0
5.	Declareren	0
6.	FI	0
7.	Juno	0
8.	NOrder	0
9.	SMART	0

ALL TIME GREATEST

1.	Apollo	0
2.	Cloud	0
3.	Connect	0
4.	Data	0
5.	Declareren*	0
6.	FI	0
7.	Juno	0
8.	NOrder	0
9.	SMART	0

Autonome development teams

Elk team is verantwoordelijk voor hun eigen Azure resources




SECUIRE SCORE
MORT9
FIGHTERS 19
MAILWARE
SCIRE
2·1·78
ERYTS
9EETA


Maandelijkse rapportage SecureScore Azure
Joost Koppers
To
Inleiding: In de schaduw van bits en bytes, waar nullen en enen dansen als onzichtbare krijgers, staan wij. Wij zijn de Secure Score Strijders, de hoeders van digitale rijken.
Onze wapens zijn geen zwaarden of schilden, maar algoritmen en firewalls. Onze missie? Bescherming bieden tegen de onzichtbare vijand: de cybercrimineel.
Daarom ga ik vanaf deze maand een maandelijkse rapportage sturen met daarin de Secure Score per subscriptie.
Net als met de kostenrapportage en onze WOC is dit hopelijk een trigger. In dit geval om actief met (informatie)beveiliging bezig te blijven.
Wie weet gaan we hier ook nog wedstrijd aan koppelen 🙂
Het streven is om alle Secure Scores op 100% te krijgen: met zinnige data.
Die laatste toevoeging staat er omdat het ook mogelijk is om alle meldingen te 'ignoren' en dan ook op 100% te komen, maar schieten we ons doel voorbij.
De Secure Score in Azure is ons kompas, onze gids door het labyrint van bedreigingen. Het is niet zomaar een getal; het is onze cyberfitheidsscore.
Hoe hoger, hoe sterker onze verdediging. Het is onze roeping om deze score te verhogen, om onze systemen te versterken en onze gegevens te beschermen.
De Vijanden: Cyberdraken en Malwaremonsters
In de diepten van het netwerk loeren ze: de cyberdraken. Ze spuwen vuur in de vorm van phishing-e-mails, ransomware en zero-day exploits. Maar wij zijn niet bang.
We hebben onze Secure Score als schild en onze kennis als wapen. We zullen niet rusten totdat elk lek is gedicht, elke kwetsbaarheid is verholpen.
De Opdracht: Verhoog de Score
Onze missie is duidelijk: verhoog de Secure Score. Elk beveiligingslek dat we dichten, elke best practice die we implementeren, brengt ons dichter bij onze overwinning.
We zullen niet rusten totdat onze score de sterren raakt, totdat onze systemen ondoordringbaar zijn.
De Toekomst: Een Veiliger Morgen
Dus sta op, Secure Score Strijders! Laat je toetsenborden ratelen als zwaarden, je muisbewegingen als dansende stappen op het slagveld.
Samen zullen we de digitale wereld veiliger maken, één regel code tegelijk. Want in deze oorlog zijn wij de helden, de verdedigers van het virtuele rijk.

Wat gebeurde er toen?

De teams gingen aan de slag

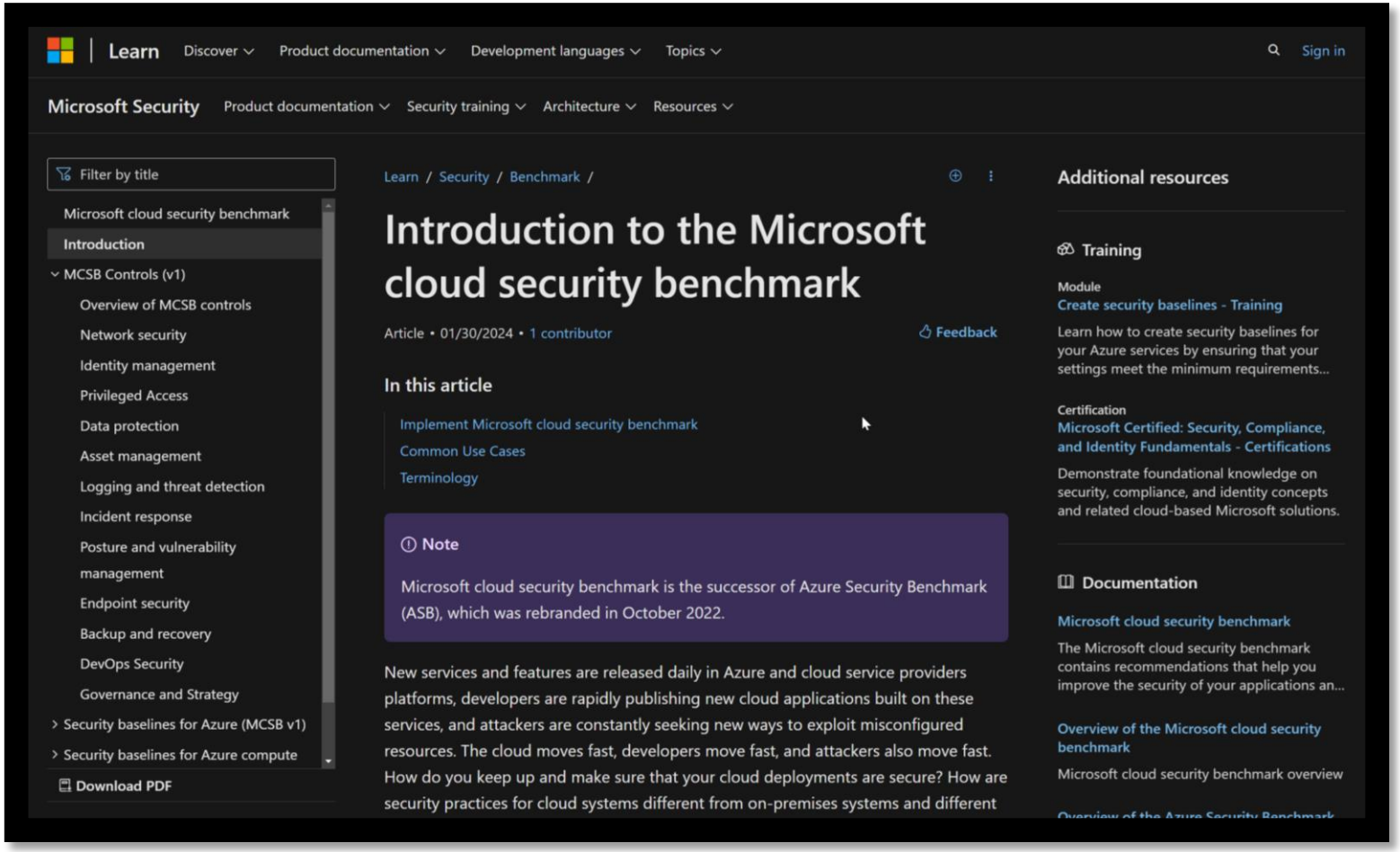
"Wij gaan dit kwartaal onze secure score met 10% verbeteren!"

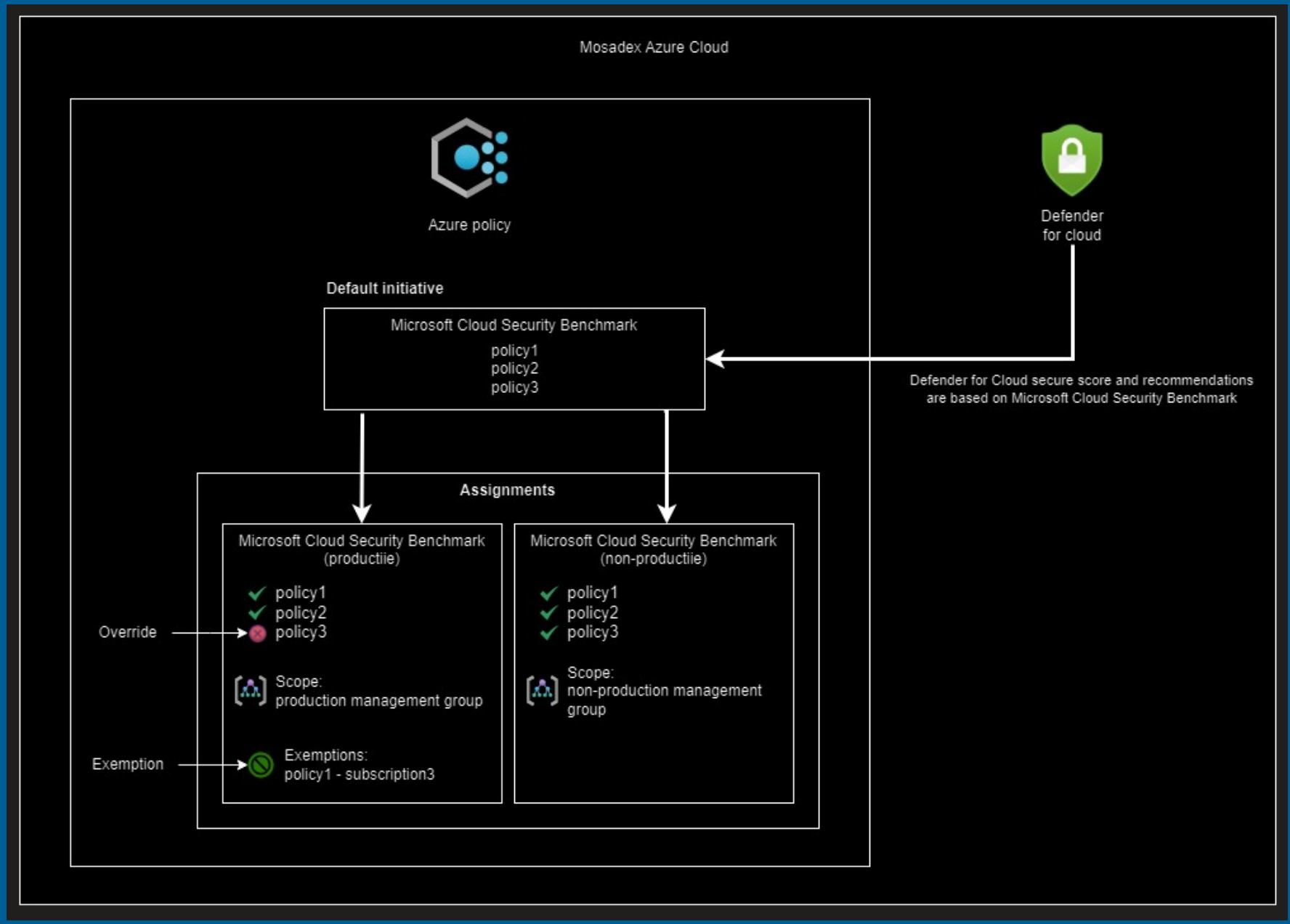
Maar we kregen ook al snel feedback…

- Sommige recommendations zijn niet relevant
- Sommige recommendations kunnen we niet zelf oplossen
  - Ligt bij het Cloud & Security team

Microsoft Cloud Security Benchmark

De Microsoft Cloud Security Benchmark ligt ten grondslag aan de Secure Score




Mosadex Azure Cloud
Azure policy
Defender
for cloud
Default initiative
Microsoft Cloud Security Benchmark
policy1
policy2
policy3
Defender for Cloud secure score and recommendations
are based on Microsoft Cloud Security Benchmark
Assignments
Microsoft Cloud Security Benchmark
(productiie)
policy1
policy2
policy3
Override
Scope:
production management group
Exemption
Exemptions:
policy1 - subscription3
Microsoft Cloud Security Benchmark
(non-productiie)
policy1
policy2
policy3
Scope:
non-production management
group

De teams gingen aan de slag

"Wij gaan dit kwartaal onze secure score met 10% verbeteren!"

Maar we kregen ook al snel feedback…

- Sommige recommendations zijn niet relevant
- Sommige recommendations kunnen we niet zelf oplossen
  - Ligt bij het Cloud & Security team

Het Cloud Governance team

Governance team

- CISO
- Enterprise architect
- Software architect

+ afvaardiging van Cloud & Security team

Het Cloud Governance proces

Governance team

Besluit welke policies wel en niet van toepassing zijn.

Development team

Lost recommendations op om Secure Score te verhogen.

Cloud & Security team

Beheert policies en exemptions in de MCSB.

Het Cloud Governance proces

Governance team

Besluit welke policies wel en niet van toepassing zijn.

Policy X is niet van toepassing

Development team

Lost recommendations op om Secure Score te verhogen.

Cloud & Security team

Beheert policies en exemptions in de MCSB.

Het Cloud Governance proces

Governance team

Besluit welke policies wel en niet van toepassing zijn.

Policy X is niet van toepassing

Policy X mag disabled worden maar alleen voor non-productie.

Development team

Lost recommendations op om Secure Score te verhogen.

Cloud & Security team

Beheert policies en exemptions in de MCSB.

Het Cloud Governance proces

Governance team

Besluit welke policies wel en niet van toepassing zijn.

Policy X is niet van toepassing

Policy X mag disabled worden maar alleen voor non-productie.

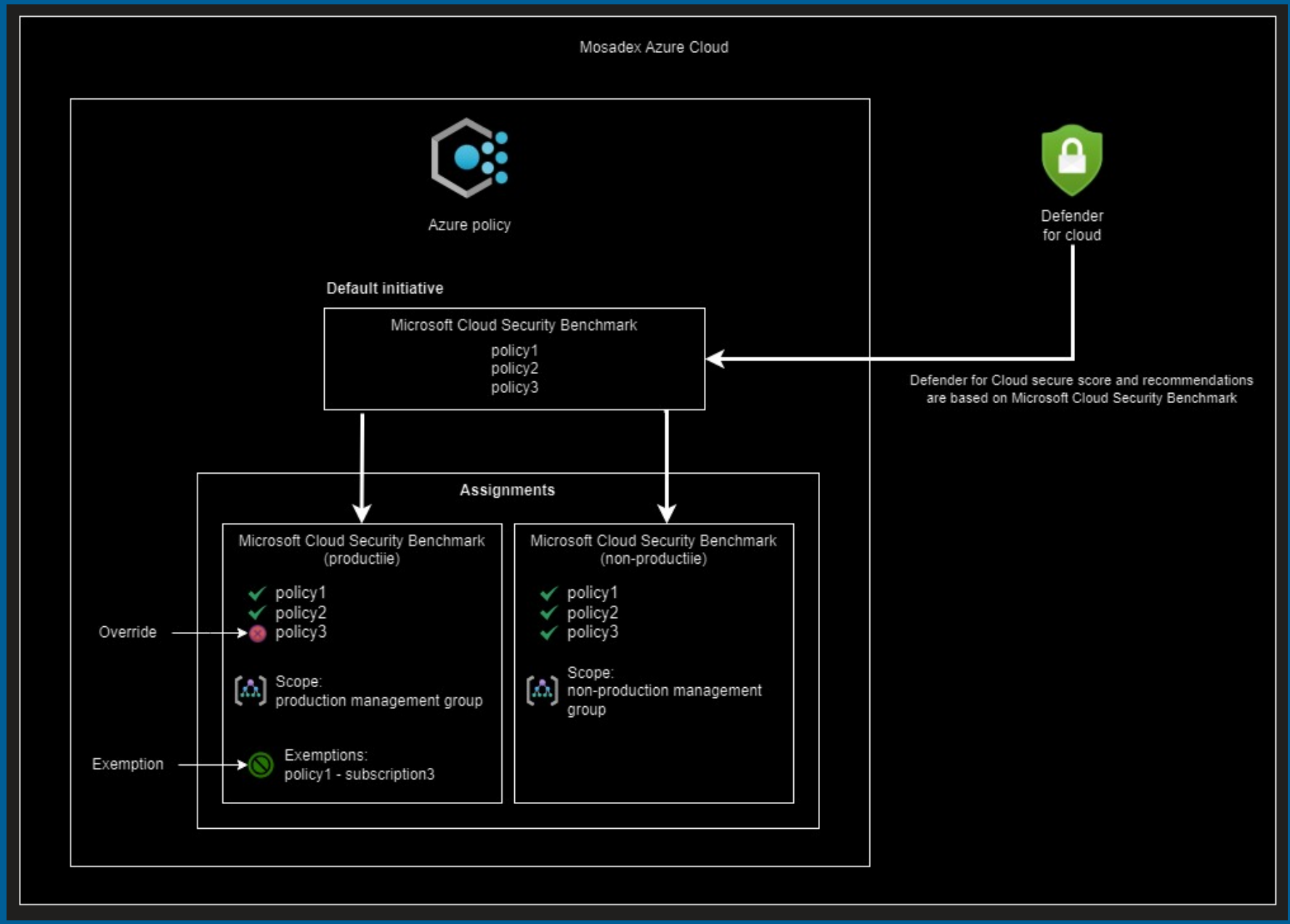
Development team

Lost recommendations op om Secure Score te verhogen.

Policy disabled, secure score omhoog.

Cloud & Security team

Beheert policies en exemptions in de MCSB.

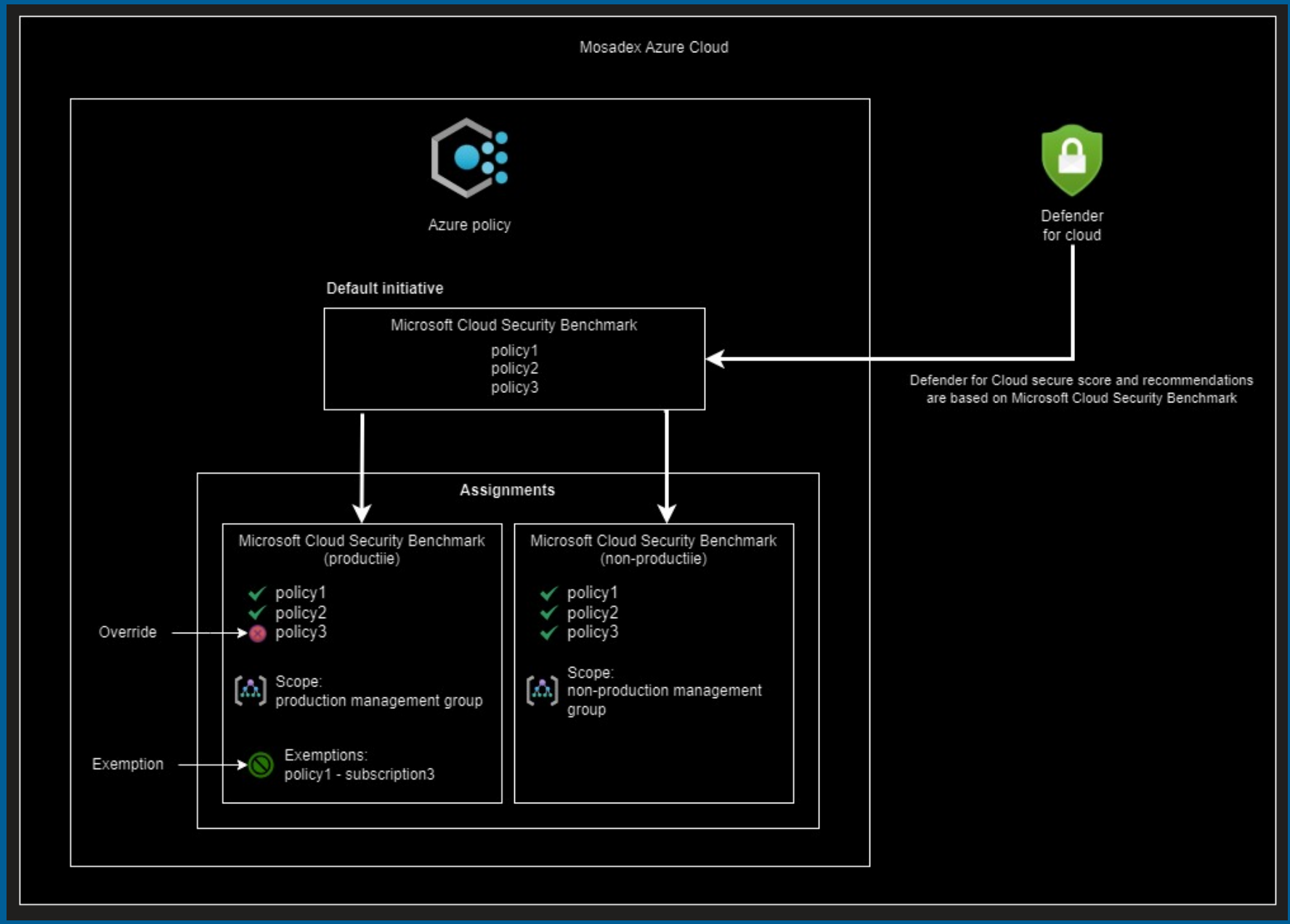

Mosadex Azure Cloud
Azure policy
Defender
for cloud
Default initiative
Microsoft Cloud Security Benchmark
policy1
policy2
policy3
Defender for Cloud secure score and recommendations
are based on Microsoft Cloud Security Benchmark
Assignments
Microsoft Cloud Security Benchmark
(productiie)
policy1
policy2
policy3
Override
Scope:
production management group
Exemption
Exemptions:
policy1 - subscription3
Microsoft Cloud Security Benchmark
(non-productiie)
policy1
policy2
policy3
Scope:
non-production management
group

Hoe houden we grip op cloud security in een organisatie met autonome development teams?

Tijdens deployment:
Azure Policies

Verschillende policy modes

- **Audit**: we kunnen zien of resources hieraan voldoen (Secure Score)
- **Disabled**: deze is niet relevant, resources hoeven hier niet aan te voldoen (weegt niet mee in Secure Score)
- **Deny**: je kunt een resource niet deployen of modifyen als die niet voldoet


Mosadex Azure Cloud
Azure policy
Defender
for cloud
Default initiative
Microsoft Cloud Security Benchmark
policy1
policy2
policy3
Defender for Cloud secure score and recommendations
are based on Microsoft Cloud Security Benchmark
Assignments
Microsoft Cloud Security Benchmark
(productiie)
policy1
policy2
policy3
Override
Scope:
production management group
Exemption
Exemptions:
policy1 - subscription3
Microsoft Cloud Security Benchmark
(non-productiie)
policy1
policy2
policy3
Scope:
non-production management
group

Grip op Cloud Security: drie fases

Vóór deployment:

Terraform Engineering standards

Tijdens deployment:

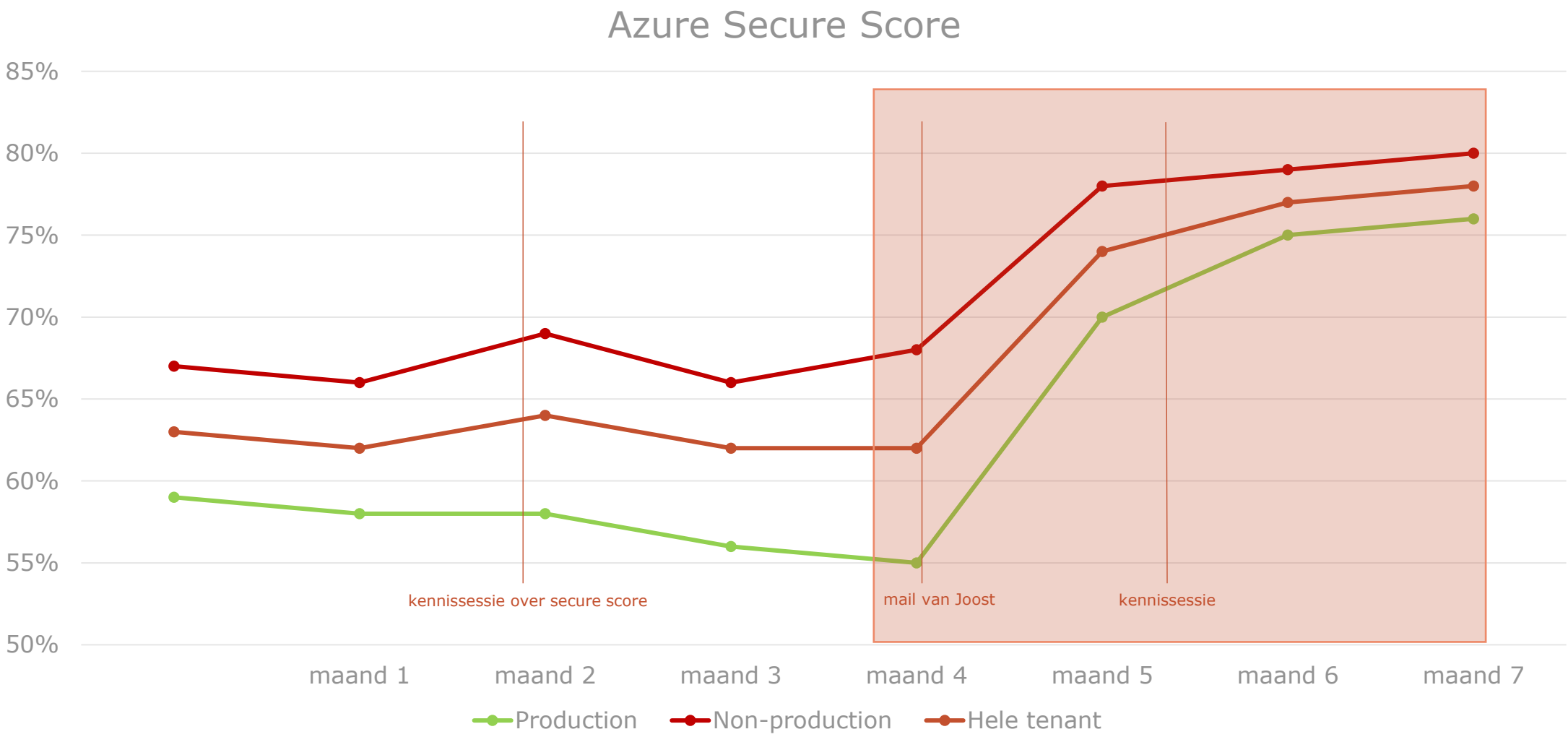
Azure policies

Na deployment:

Secure Score in Defender for Cloud

Heeft het gewerkt?

De secure score ging omhoog!



Wat hebben we geleerd?

Lessons Learned

Houd Cloud Security leuk…

- Maak het meetbaar
- Maak er een wedstrijdje van!

je recommendations relevant…

- Disable policies die niet passen
- Sta open voor feedback

en je Secure Score hoog!

- Blijf er aandacht aan besteden
- Gebruik Deny policies

Bedankt voor jullie aandacht!

Vragen?