APS IT diensten

Voor ICT in het belang van je school

Professionaliseringsdag

The state of the world & Zero Trust

Tony Krijnen

AKA.MS/LINKTONY

(Link naar slides zit aan het einde)

Nationaal Cyber Security Centrum – Cybersecuritybeeld 2023

https://www.ncsc.nl/onderwerpen/cyber-security-beeld-nederland

Home > Onderwerpen > **Cybersecuritybeeld Nederland**

Publicatie | 03-07-2023

› Cybersecuritybeeld Nederland 2023

Publicatie | 03-07-2023

Microsoft Digital Defense Report

https://www.microsoft.com/en-us/security/security-insider/microsoft-digit...

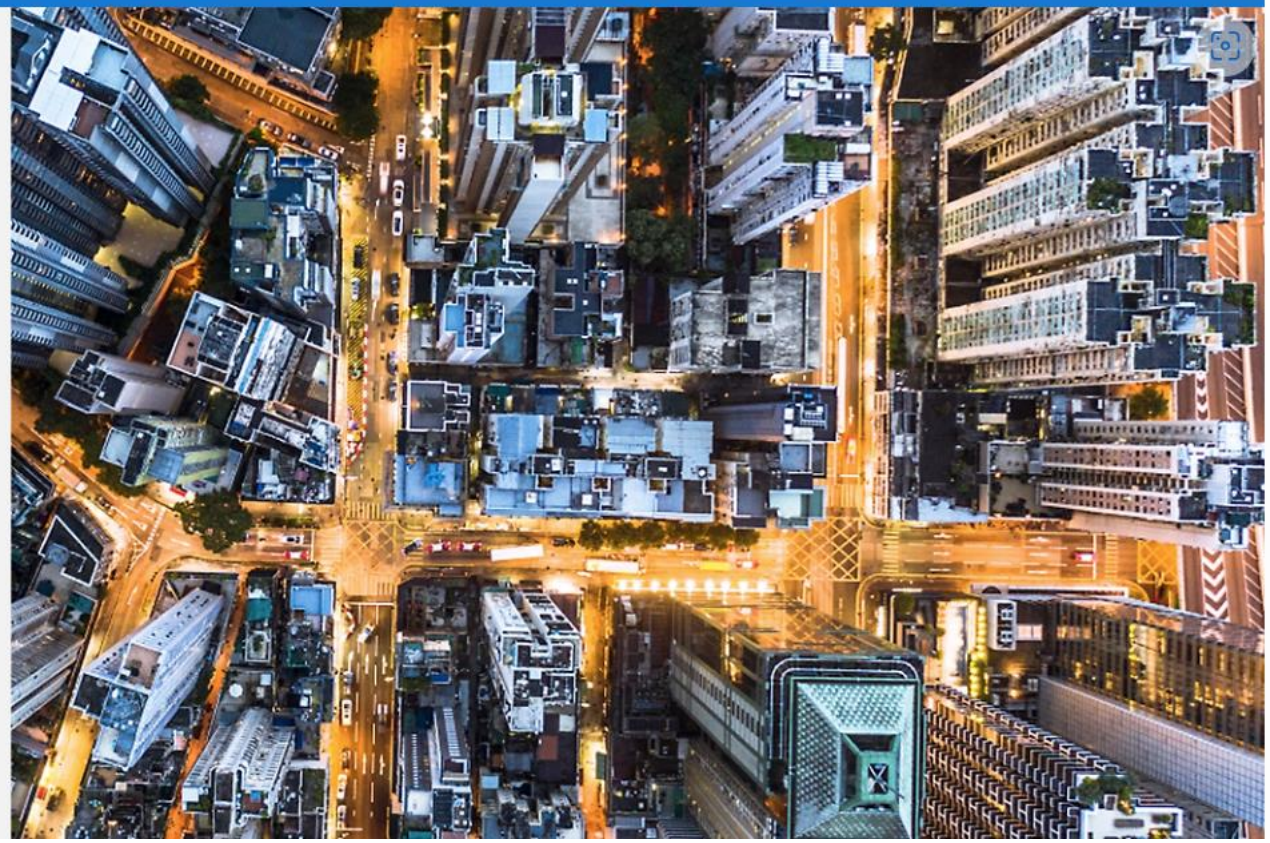
Microsoft | Microsoft Security Solutions Products Services Partners Resources Contact Sales Start free trial All Microsoft

Security Insider Threat Briefs Reports Behind the scenes Threat actor insights

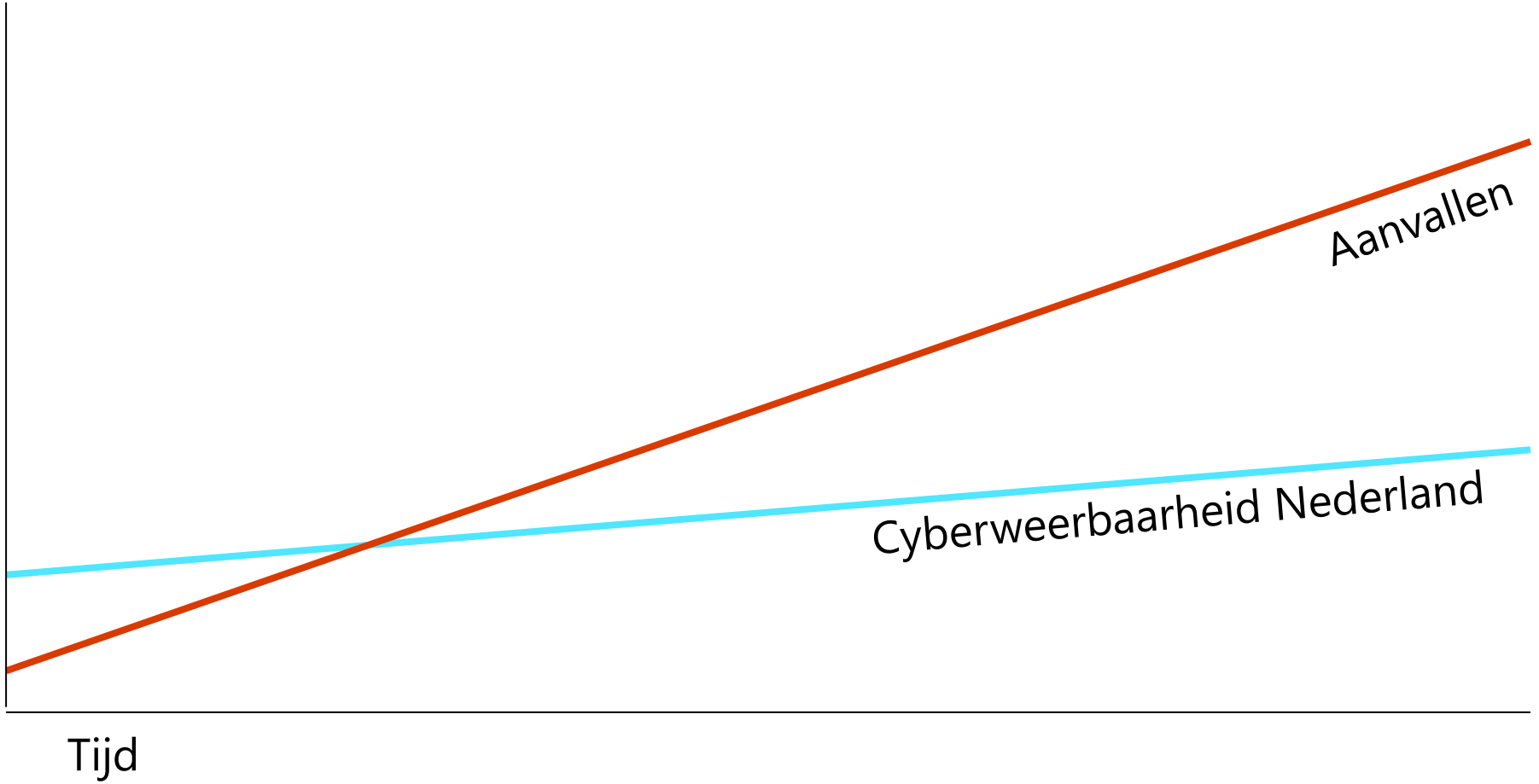
The State of Cybercrime

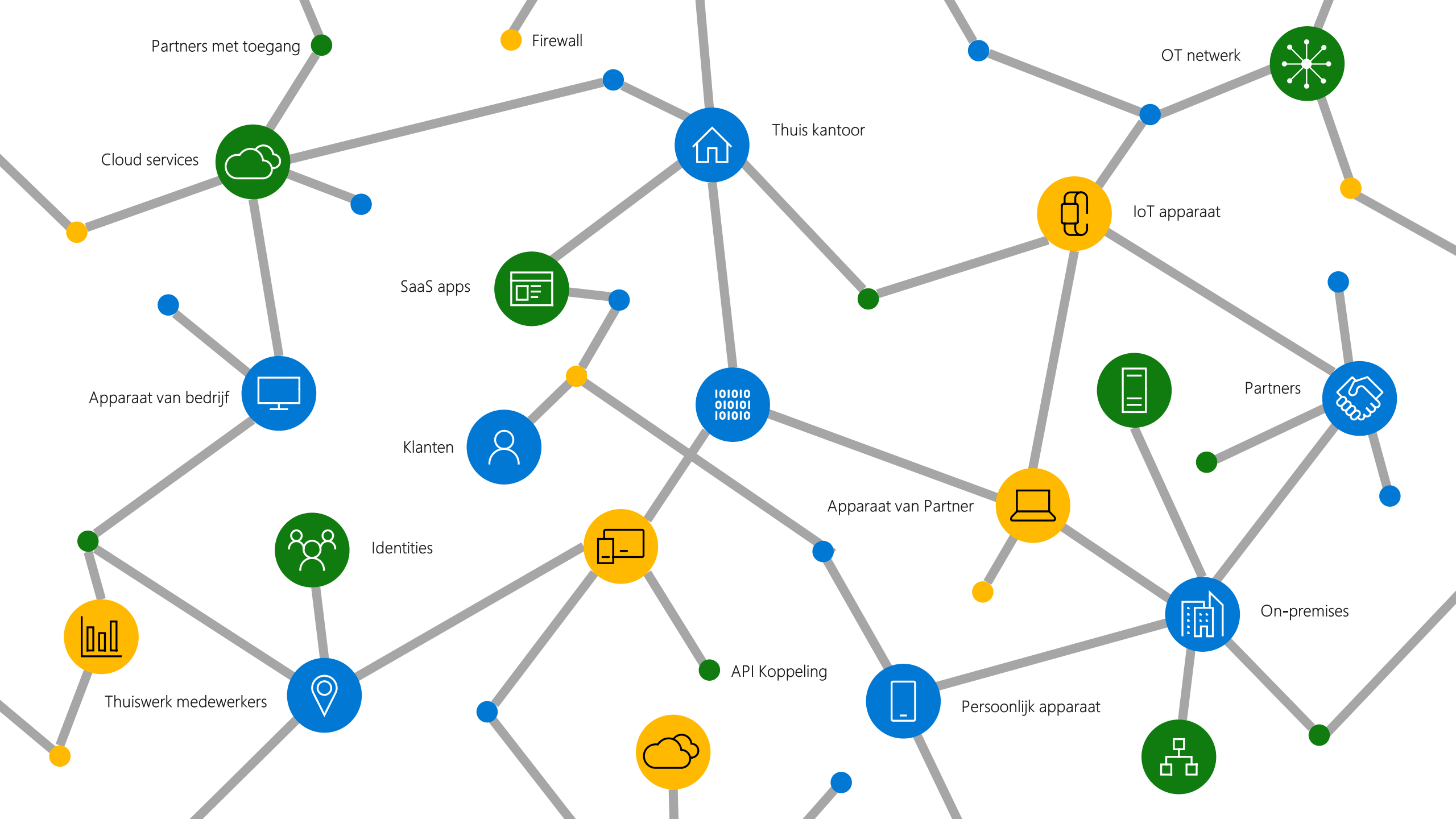
As cyber defenses improve and more organizations are taking a proactive approach to prevention, attackers are adapting their techniques.

Download the report Download the Executive summary



Cyberweerbaarheid vs aanvallen




Partners met toegang
Firewall
OT netwerk
Cloud services
Thuis kantoor
IoT apparaat
SaaS apps
Apparaat van bedrijf
Partners
Klanten
Apparaat van Partner
Identities
On-premises
Thuiswerk medewerkers
API Koppeling
Persoonlijk apparaat

De evolutie van de aanvallers

- Big Business, dit is echt een industrie
- Heeft echt bedrijfsmanagement
- Landen die actief aan Cybercrime doen, Cybercrime Syndicates
- Enorme investeringen, Automatisering, gebruik van AI (Maar AI zal verdedigers ook helpen)

De menu kaart van cybercriminals

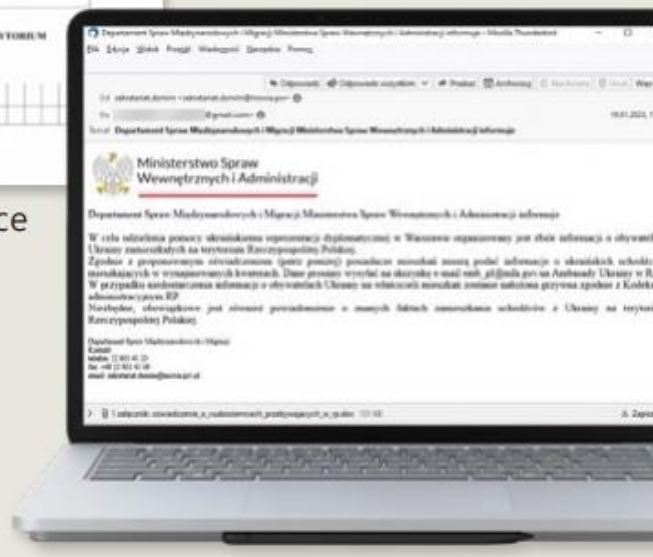
- Cybercrime-as-a-Service
- Phising-as-a-Service
- Ransomware-as-a-Service
- Cryptojacking
- Beinvloeden van mensen

Dissemination tactics in Poland

Real world and digital campaigns converged on Poland, where fliers with a QR code posted throughout Polish cities and attachments in mass email campaigns led to the same document demanding the PII of Ukrainian refugees. Polish civilians received the same message from multiple angles, which likely reinforced its perception as legitimate.

Real world messaging

Real world convergence



Digital world messaging

Data from Microsoft on Cybersecurity

65 biljoen
signalen dagelijks gesynthetiseerd

Dat is meer dan 740 signalen per seconde, gecombineerd door geavanceerde data-analyse en AI-algoritmes. Hiermee krijgen we inzicht in de digitale bedreigingen en cybercriminaliteit.

10.000+
experts op beveiliging en bedreigingsinformatie

10.000+ ingenieurs, onderzoekers, datawetenschappers, cyber-beveiligingsexperts, threat hunters, geopolitieke analisten en eerstelijnsrespondenten over de hele wereld

4.000
identity aanvalen worden geblokeerd per seconde

4.000 bedreigingen op identiteit en authenticatie gestopt per seconde

15.000+
partners in ons security ecosysteem

15.000 partners met gespecialiseerde oplossingen in ons beveiligings-ecosysteem verhogen de cyber-weerbaarheid van onze klanten

300+
bedreigingsactoren gevolgd

Microsoft Threat Intelligence is gegroeid om meer dan 300 unieke bedreigingsactoren te volgen, waaronder 160 nationale actoren, 50 ransomwaregroepen en honderden anderen

100.000+
domeinnamen verwijderd

100.000+ domeinnamen die werden gebruikt door cybercriminelen (inclusief meer dan 600 domeinnamen van nationale actoren)

135 miljoen
beheerde apparaten

135 miljoen beheerde apparaten geven inzichten in de beveiliging en bedreigingen

The State of Cybercrime: key developments

80-90%

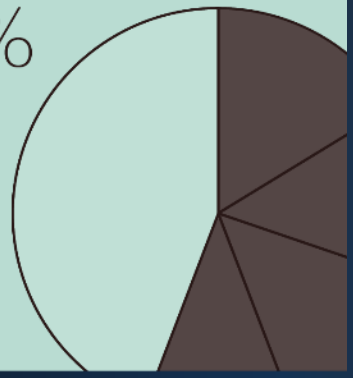
van de succesvolle ransomware aanvallen begonnen in apparaten die niet beheerd werden

70%

van de organisaties die met human-operated ransomware te maken kregen hadden minder dan 500 medewerkers

Human-operated ransomware aanvallen stegen met

200%



Het rendement op mitigatie (ROM) is handig voor prioritering en kan acties benadrukken die weinig inspanning of middelen vereisen, maar een grote impact hebben

Wachtwoord aanvallen stegen sterk in 2023

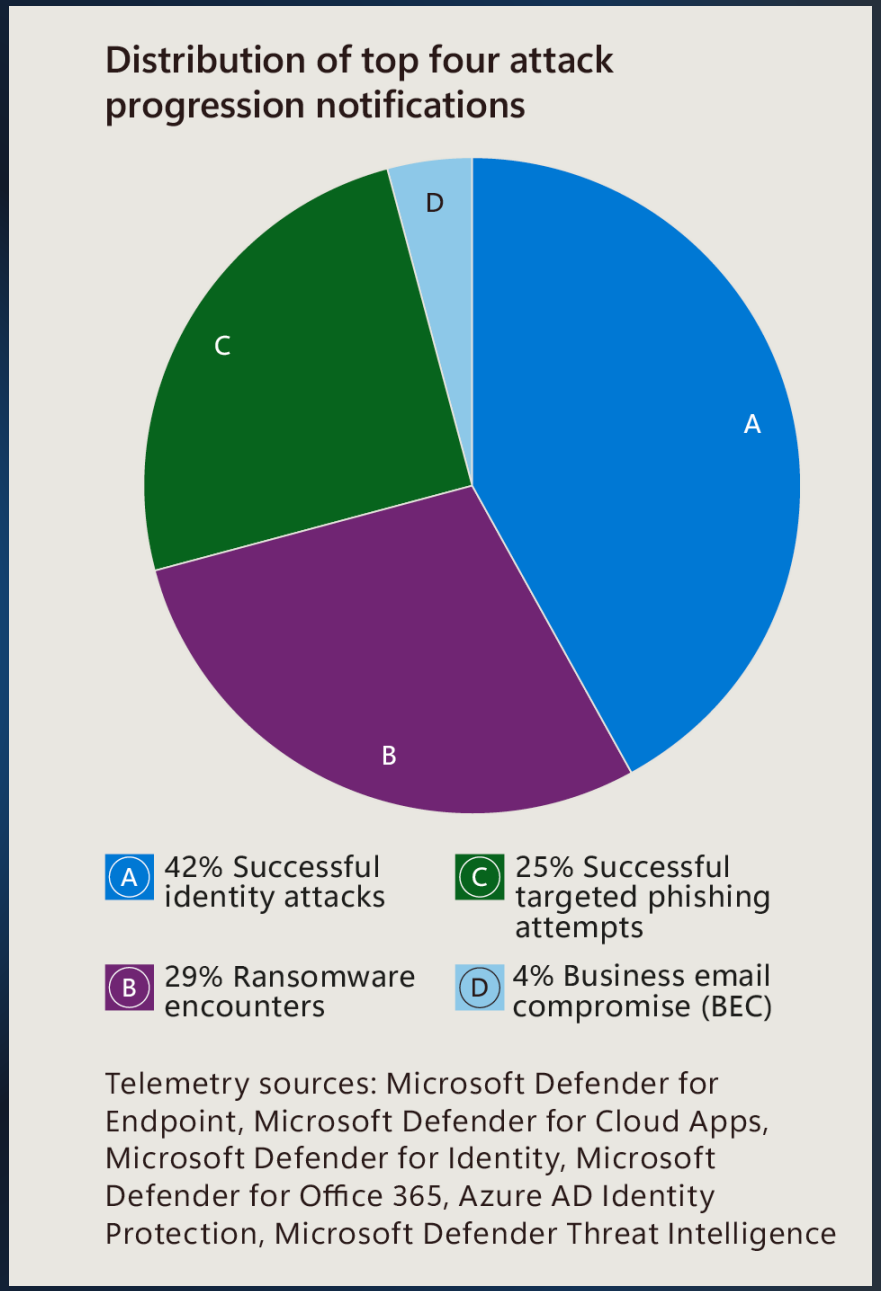
Afgelopen jaar markeerde een belangrijke verschuiving in de tactieken van cybercriminelen.

met dreigingsactoren die Cloud computing resources zoals virtuele machines misbruikten om DDos-aanvallen te lanceren. Wanneer honderden miljoenen verzoeken per seconde afkomstig van tienduizenden apparaten een aanval vormen, is de Cloud onze beste verdediging, vanwege de schaal die nodig is om deze grote aanvallen te af te slaan.

Wat zien wij in de meldingen aan aanvallen?

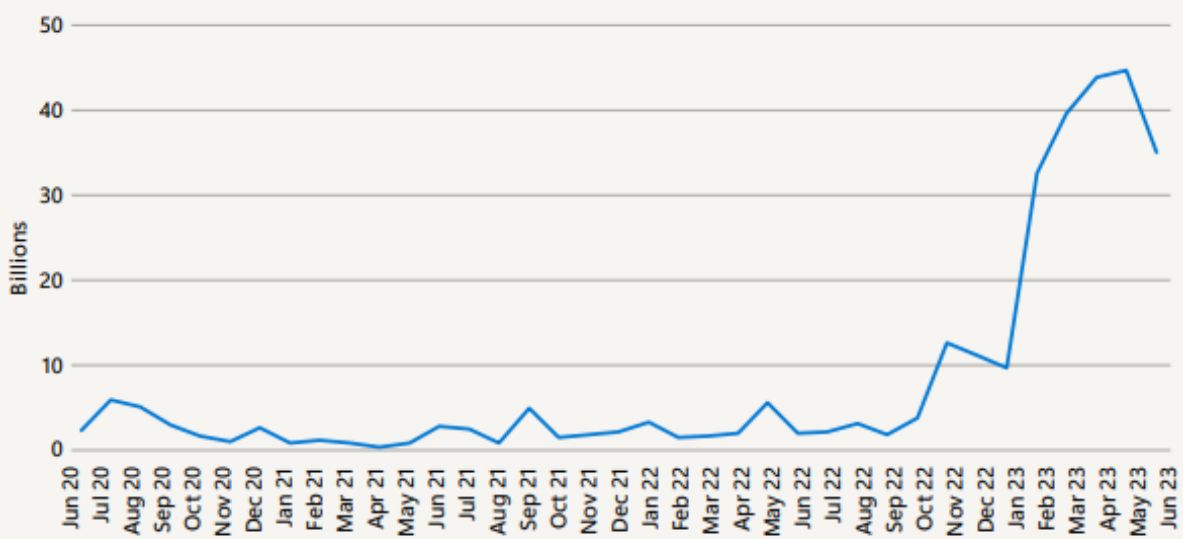
Op basis van de meldingen die met klanten zijn gedeeld, zijn dit de belangrijkste bedreigingen die dit jaar door Microsoft Defender Experts zijn geïdentificeerd:

- Succesvolle identiteitsaanvallen
- Ransomware aanvallen
- Gerichte phishing pogingen die leiden tot het compromitteren van apparaten of gebruikers
- Compromitteren van zakelijke e-mail



Inzichten op identiteit aanvallen

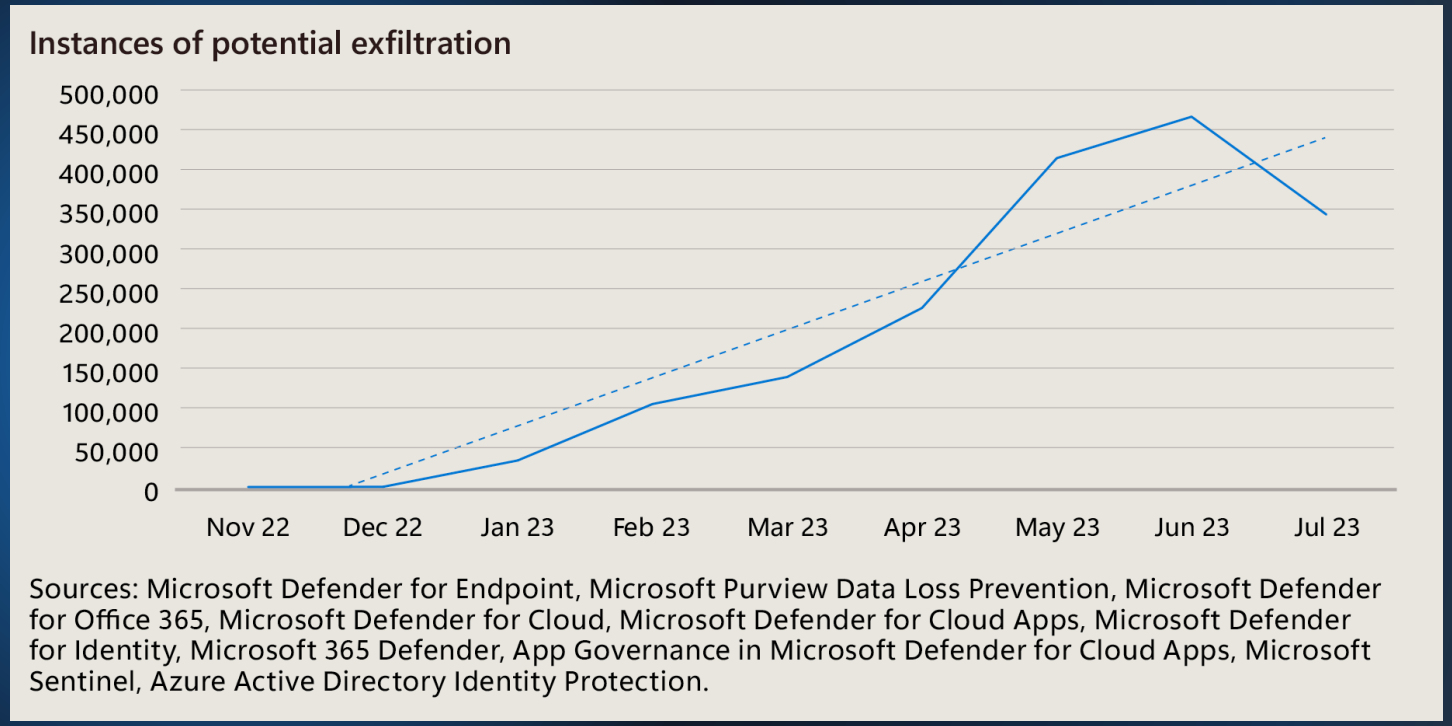
- Eenmalige wachtwoordbots
- Multifactor authentication (MFA) vermoeidheid is een bedreiging
- Token replay blijft een veel voorkomende bedreiging



Bron: Microsoft Entra data

Inzichten over Ransomware en afpersing

- >200% toename van ransomware-aanvallen die door mensen worden uitgevoerd
- 13% van de ransomware-aanvallen nu data-exfiltratie
- 70% van de succesvolle aanvallen zijn gericht tegen organisaties met <500 werknemers
- Trend in versleuteling op afstand
- 80-90% van de succesvolle aanvallen vindt zijn oorsprong via onbeheerde apparaten



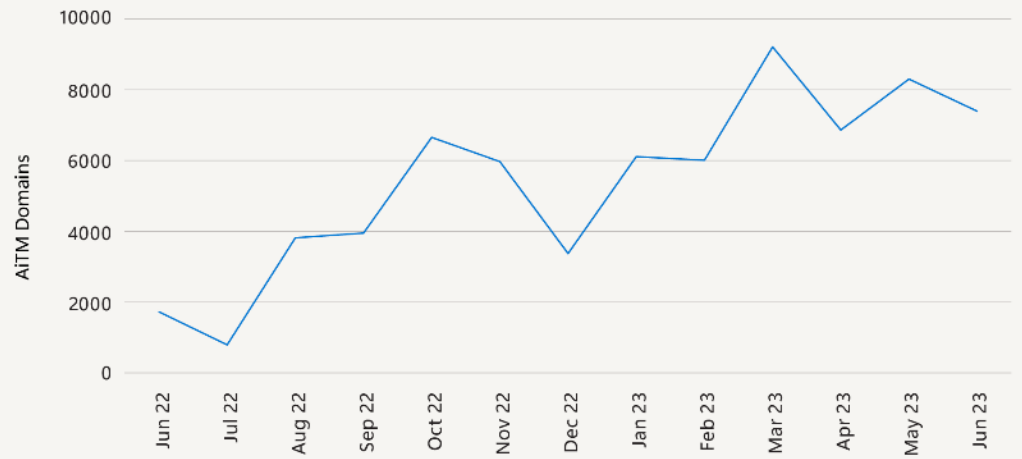
Sources: Microsoft Defender for Endpoint, Microsoft Purview Data Loss Prevention, Microsoft Defender for Office 365, Microsoft Defender for Cloud, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft 365 Defender, App Governance in Microsoft Defender for Cloud Apps, Microsoft Sentinel, Azure Active Directory Identity Protection.

Inzichten over Phishing

- Phishing technieken evolueren (Qphising)
- Adversary-in-the-middle (AiTM) attacks
- Caffeine, EvilProxy, NakedPages vs EvilGinx2, Modlishka

AiTM domains growing as attacks become more common

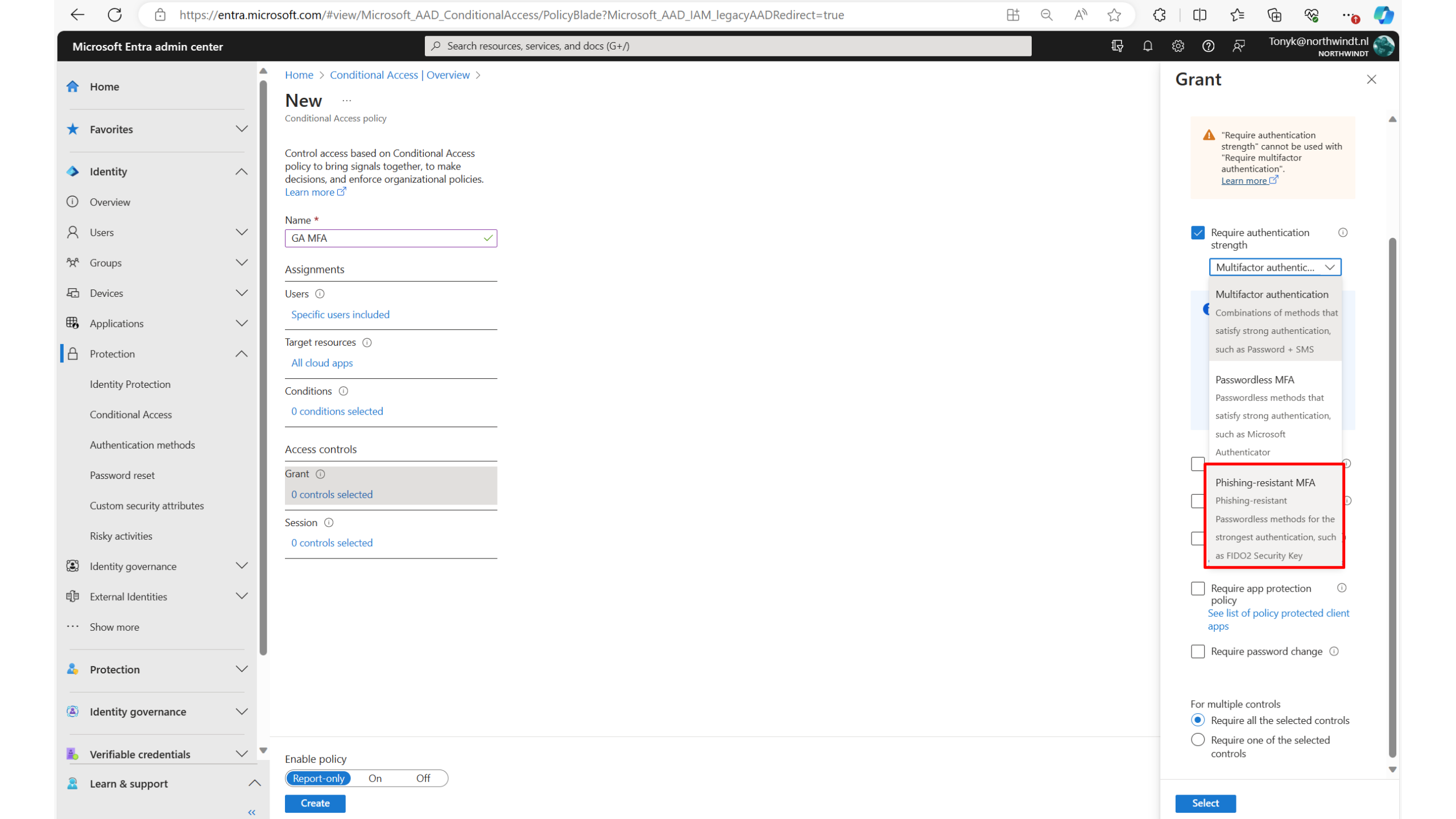
The number of domains that we tracked leading to AiTM phishing pages grew consistently throughout the last 12 months



Source: Microsoft Defender for Office 365

10,000

In April-June 2023 we alerted users of approximately 10,000 password entries per month into malicious sites.


https://entra.microsoft.com/#view/Microsoft_AAD_ConditionalAccess/PolicyBlade?Microsoft_AAD_IAM_legacyAADRedirect=true
Microsoft Entra admin center
Search resources, services, and docs (G+/)
Tonyk@northwindt.nl
NORTHWINDT
Home
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity Protection
Conditional Access
Authentication methods
Password reset
Custom security attributes
Risky activities
Identity governance
External Identities
Show more
Protection
Identity governance
Verifiable credentials
Learn & support
Home > Conditional Access | Overview >
New
Conditional Access policy
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more
Name *
GA MFA
Assignments
Users
Specific users included
Target resources
All cloud apps
Conditions
0 conditions selected
Access controls
Grant
0 controls selected
Session
0 controls selected
Enable policy
Report-only
On
Off
Create
Grant
"Require authentication strength" cannot be used with "Require multifactor authentication".
Learn more
Require authentication strength
Multifactor authentic...
Multifactor authentication
Combinations of methods that satisfy strong authentication, such as Password + SMS
Passwordless MFA
Passwordless methods that satisfy strong authentication, such as Microsoft Authenticator
Phishing-resistant MFA
Phishing-resistant Passwordless methods for the strongest authentication, such as FIDO2 Security Key
Require app protection policy
See list of policy protected client apps
Require password change
For multiple controls
Require all the selected controls
Require one of the selected controls
Select

Inzichten over zakelijke e-mail compromitteren

- Financiële fraude
- Laterale beweging door interne phishing

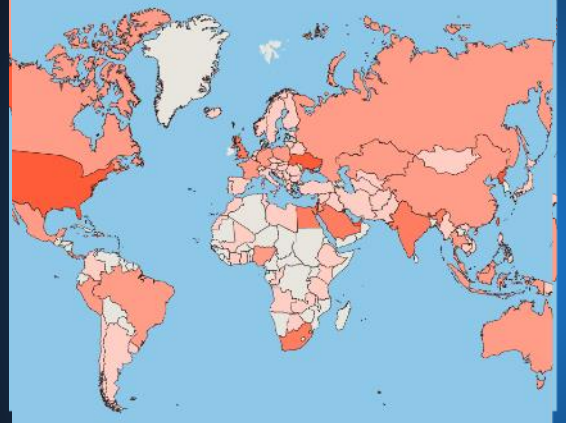
Hoe BEC evolueert:

- Uitgebreid misbruik van Cloud gebaseerde infrastructuur
- Misbruik maken van vertrouwde zakelijke relaties: e-mail compromitteren van leveranciers, klanten
- Aanvallers investeren veel in kennis
- Aanvallers delen onderling actief informatie

Nation State bedreigingen

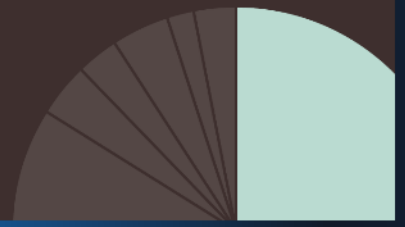
Nation-state bedreigingen:
Belangrijkste ontwikkelingen

De activiteiten van natiestaten en aan de staat gelieerde dreigingsactoren gingen weg van zo veel mogelijk destructieve aanvallen naar spionagecampagnes.



De ongecontroleerde uitbreiding van de markt voor cyberhuurlingen dreigt de bredere online omgeving te destabiliseren

Door de Russische staat gesponsorde dreigingsactoren gebruikten verschillende middelen om toegang te krijgen tot apparaten en netwerken in NAVO-lidstaten.



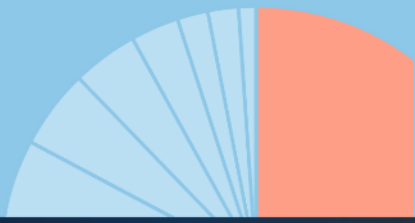
Iraanse staatsactoren maken gebruik van steeds geavanceerdere handelspraktijken

including enhancing operations in cloud environments, regularly using custom implants, and exploiting newly released vulnerabilities faster.

Chinese dreigingsactoren voeren complexe en geavanceerde wereldwijde informatie collectie campagnes uit.

At the same time, China's cyber influence campaigns continue to operate at an unmatched scale.

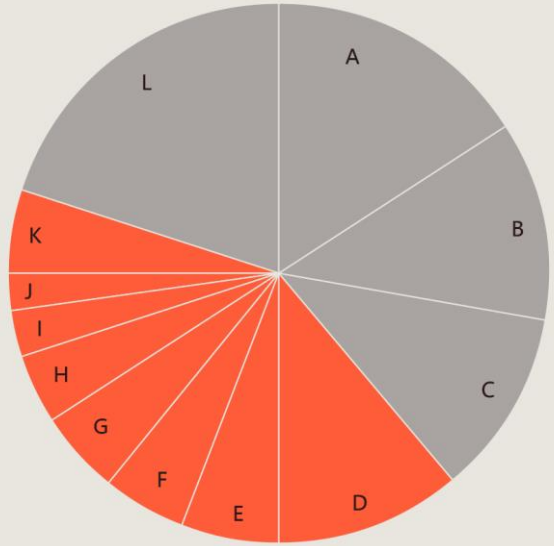
Actoren in Noord-Korea voerden een aanval op de toeleveringsketen uit met behulp van een bestaand beveiligingslek in de toeleveringsketen



Een groeiende focus op kritieke infrastructuur

Most targeted sectors globally

State-sponsored threat groups target broadly as part of their intelligence collection. Critical infrastructure sectors (highlighted) comprised 41% of the NSNs sent in FY2023.



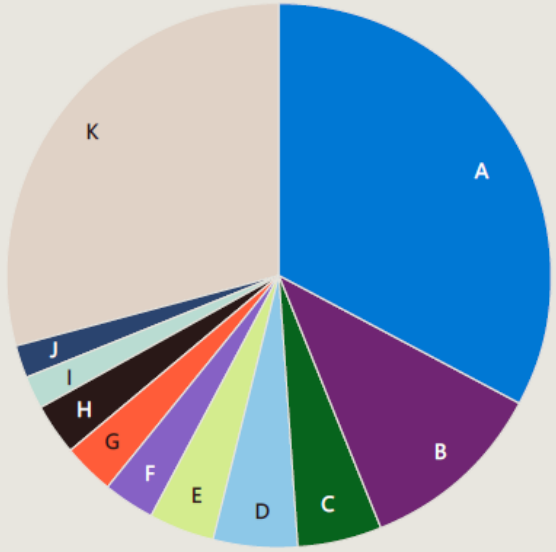
- A 16% Education
- B 12% Government
- C 11% Think tanks and NGOs
- D 11% IT
- E 6% Communications
- F 5% Finance
- G 5% Transportation
- H 4% Defense Industry
- I 3% Energy
- J 2% Manufacturing Infrastructure
- K 5% Other Critical Infrastructure
- L 20% Other

Source: Microsoft Threat Intelligence NSN data.

Most targeted regions in Europe

From all attacks on Europe
The Netherlands had 3%

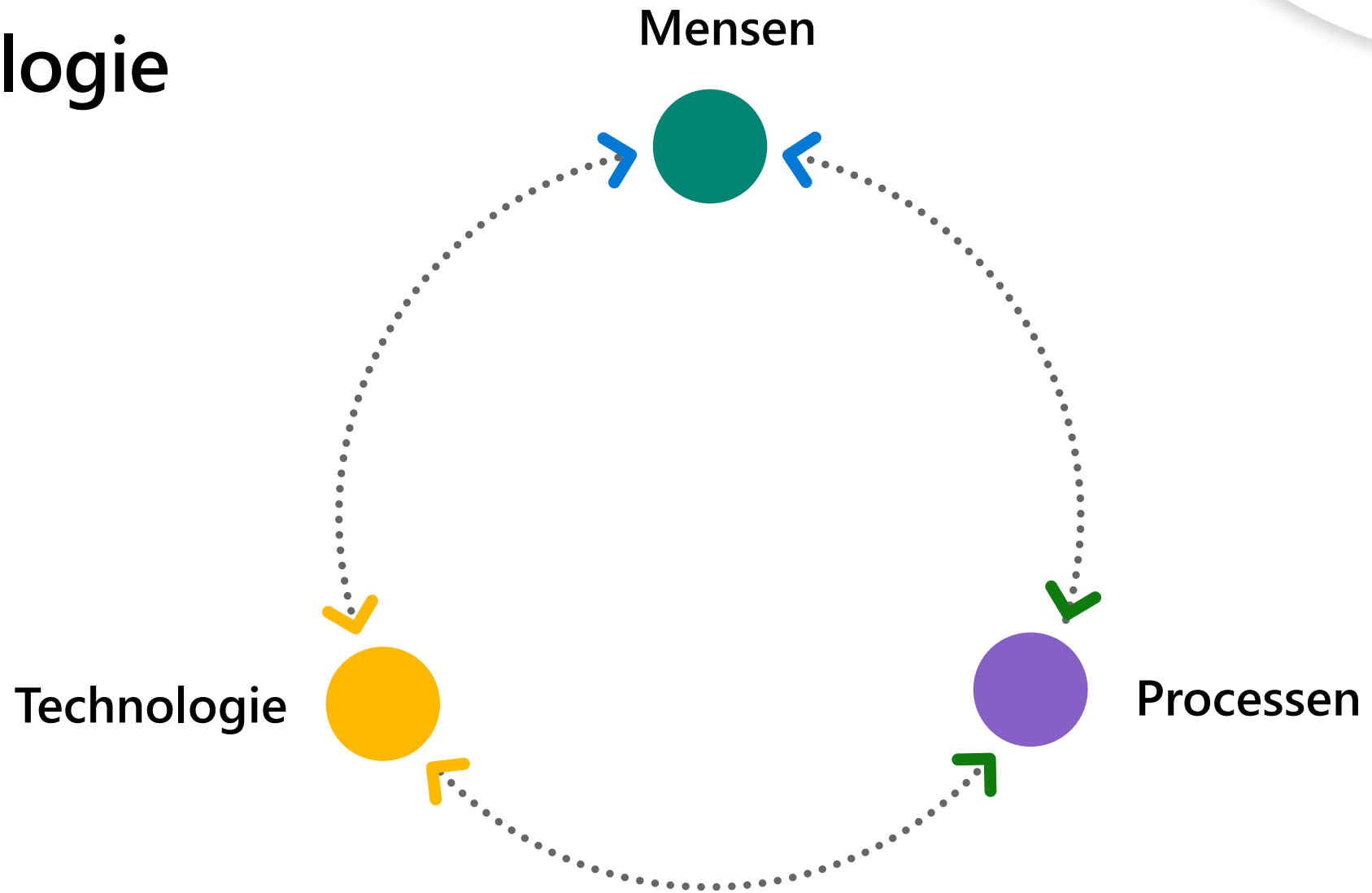
Europe



- A 33% Ukraine
- B 11% United Kingdom
- C 5% France
- D 5% Poland
- E 4% Italy
- F 3% Germany
- G 3% Switzerland
- H 3% Netherlands
- I 2% Azerbaijan
- J 2% Albania
- K 29% Other

Hoe kunnen we ons beschermen tegen 99% van de aanvallen?

Meer dan technologie




BRAND!

Call to action

1) Zorg voor Phising Resistent MFA voor (Global) admin accounts
2) **Alle users** moeten MFA hebben.
3) Waar ligt ons draaiboek voor als we een aanval hebben?
4) Hebben we XDR of hebben we point solutions?
5) Bij Azure abonnementen: Blokkeer resources die je niet wilt met Azure Policies

Microsoft

Thank you

https://aka.ms/ZeroTrustNis2
https://aka.ms/NIS2TM

AKA.MS/HYPER-T

APS IT-diensten
Voor ICT in het belang van je school

APS IT-diensten
Zwarte Woud 2
3524 SJ Utrecht

www.apsitdiensten.nl

T 030 2856 870
M info@apsitdiensten.nl