previder

Even voorstellen

Marco Vader

Consultant Informatiebeveiliging || Coördinator Security Operations

m.vader@previder.nl

it starts here.

Managed Detectie & Response (MDR)

- Risicobeheersing
- Maatregelen versus beleid
- MDR/SIEM/SOC als maatregel
- Voorbeelden MDR/SIEM/SOC

it starts here.

Zomaar een paar getallen

98% … van de cyberincidenten (datalekken en ransomware) is er sprake van menselijke fouten

96% … van de phishing aanvallen komt per e-mail binnen

51% … krijgt te maken met een ransomware aanval

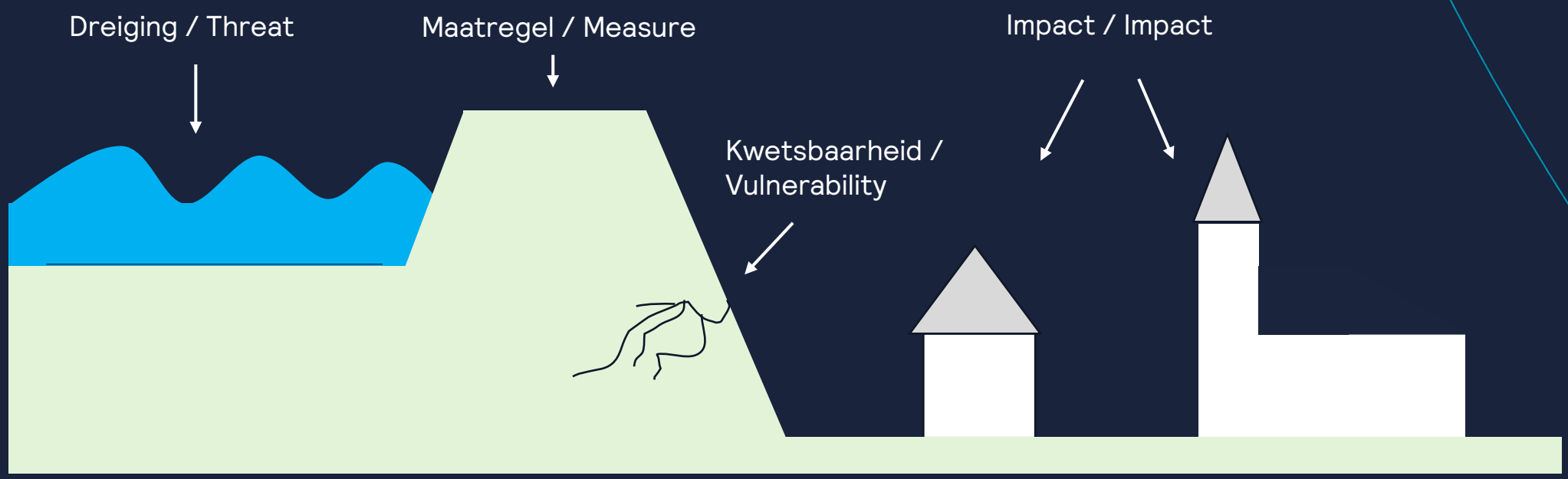
25% … van alle datalekken is er sprake van phishing

20% … van de datalekken ontstaat door verloren of gestolen inloggegevens

NIS2 Per oktober 2024 is de NIS2 wetgeving van toepassing

previder

IT Security & IB | De basis = risicomanagement

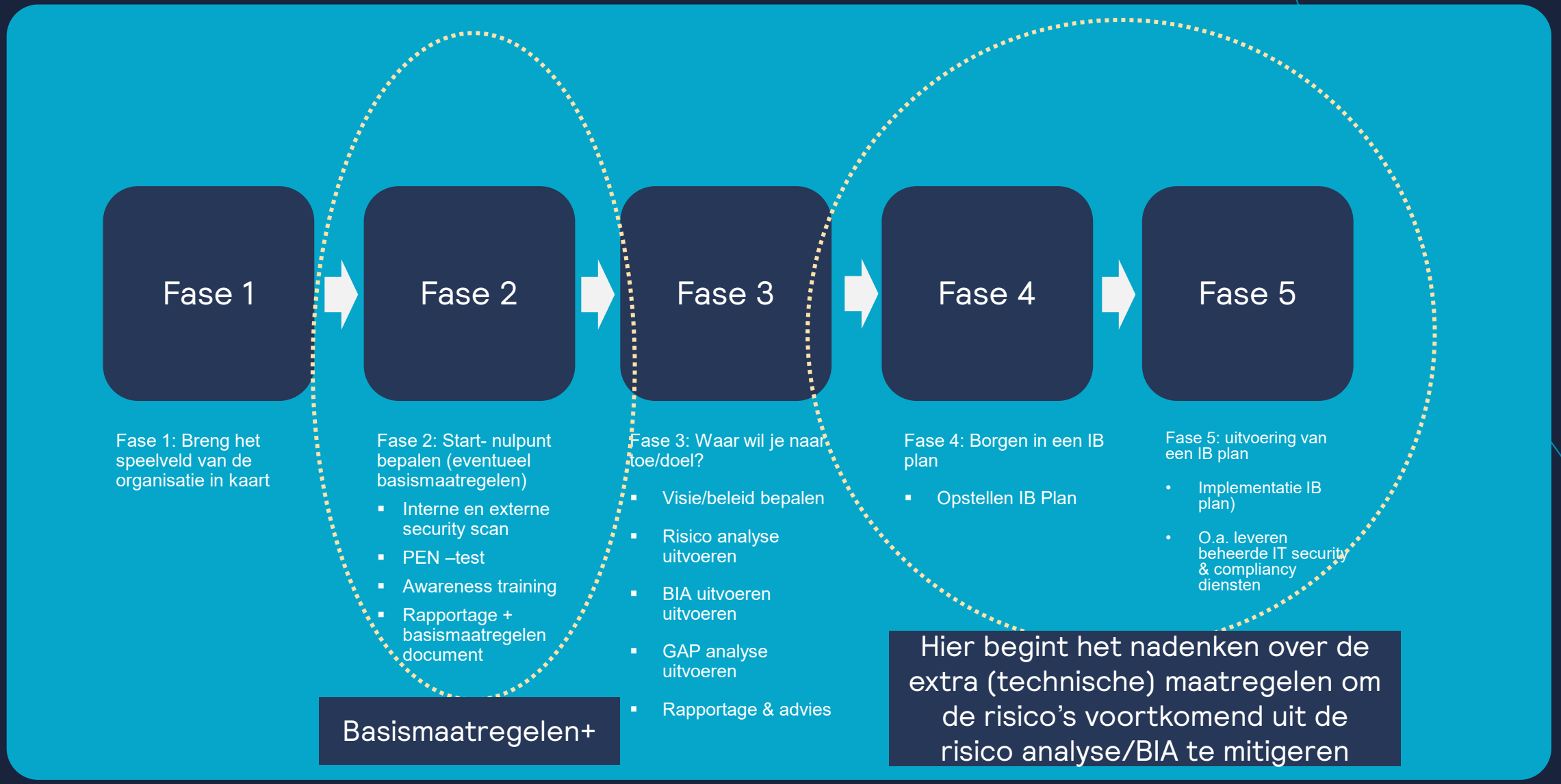


Risico = Impact * Kans

previder

it starts here.

Wanneer is het juiste moment om over maatregelen na te denken?



Begin bij de basismaatregelen

- Bewustwording creëren (door bijv. awareness training);
- IAM: MFA/WW beleid/role based & conditional access etc;
- Preventieve maatregelen: anti-virus/malware, firewall;
- Back-up;
- O.S. beheer: hardening, patching/updates;
- Netwerksegmentatie;
- Dienstbeschrijvingen + SLA's met ketenleveranciers;

MDR: Waarom detectie & response?

previder

it starts here.
it starts here.

IT security gelaagdheid | preventie vs detectie & reactie

Preventie

(traditionele preventieve maatregelen)

- Anti Virus, Firewall
- MFA, Role based access
- Awareness training

Detectie & Reactie & Herstel

(EDR/MDR/xDR)

- Detectie, reactie en maatregelen nemen
- Threat hunting (gevaar voorspellen)
- Forensics (opsporing oorzaak na incident)

Fundament op orde → IB volwassenheid niveau 5

Afkortingen en terminologieën

EDR vs MDR vs XDR

Endpoint Detection and Response (EDR) = detecteert bedreigingen en hierop kan reageren.

Het is bedoeld om de tekortkomingen van traditionele (eindpunt)beschermingsoplossingen te compenseren wat betreft het voorkomen van alle aanvallen.

Managed Detectie & Response (MDR) = EDR + pro actieve monitoring + reactie + herstel

Extended Detectie & Response (XDR) = MDR over verschillende security domeinen.

SIEM/SOAR/EABU/AI

Tools om MDR/XDR te gebruiken/optimaliseren/automatiseren

Enkele detectie & response bouwstenen

Identity
On-prem | Private Cloud

Lokale Identity Sensor

Identity
Azure AD | Microsoft 365

Identity Azure AD

Endpoint
Eindgebruikers devices
- Windows | Linux |
- MacOS

EDR clients

Servers
Servers
- Azure | On-prem | Private cloud
- Windows | Linux

EDR Servers

Microsoft 365

Office 365
- SharePoint
- Teams
- Exchange

Vulnerability Management
- Servers
- Clients
- Firewalls
- Applicaties
- Services

+SIEM=MDR

previder

it starts here.

it starts here.

SOC - bouwstenen

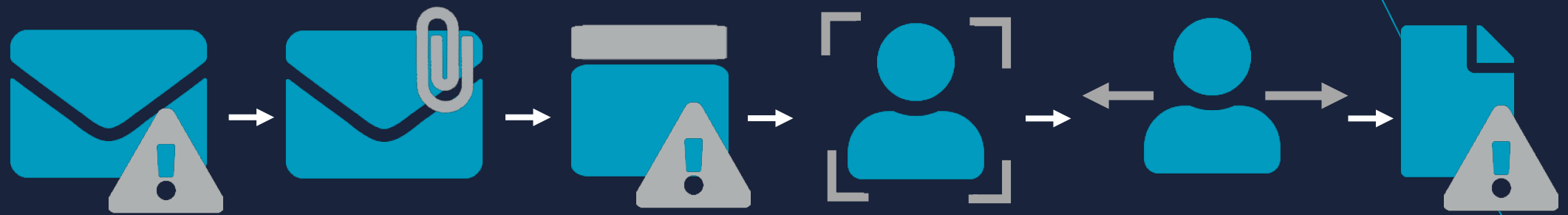
Data collecting & continuous **monitoring**

Use cases & correlation

Analyse, hunting, response, forensics

Sec. Ops. portfolio

Voorbeeld MDR toepassing



Phishing mail

Bijlage wordt geopend

Malware wordt geïnstalleerd

Aanvaller neemt het account over

Aanvaller krijgt toegang tot meer systemen

Aanvaller verkrijgt en steelt data

mail security

awareness

MDR end-point

MDR identity

MDR servers & applicaties

maatregelen

Restrisico

Restrisico

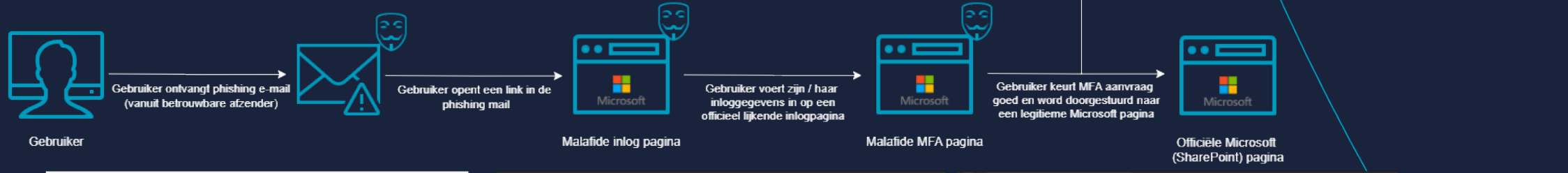
Restrisico

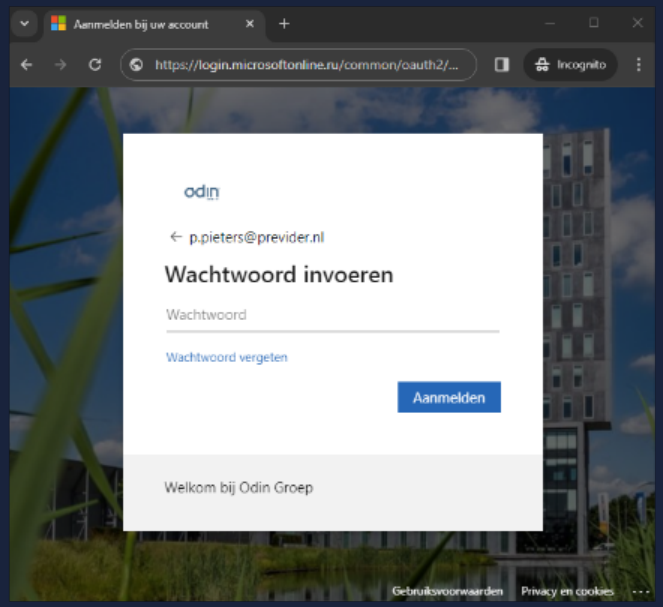
Restrisico

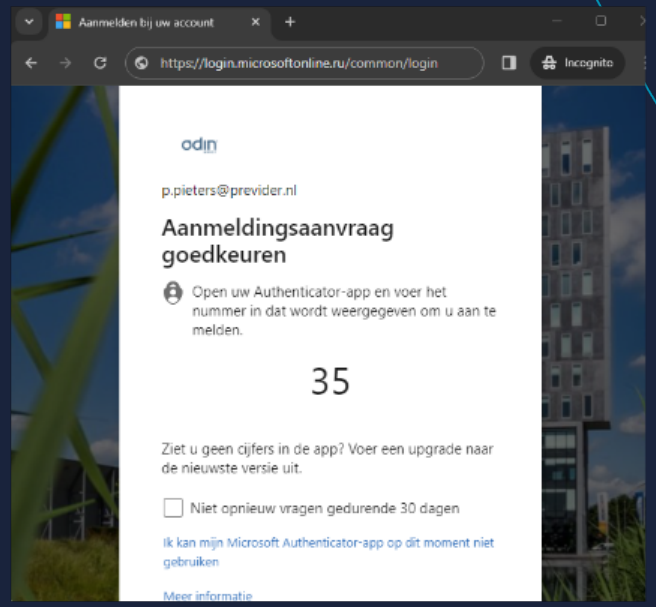
Restrisico

Restrisico

Hoe hackers MFA kunnen omzeilen (AiTM)



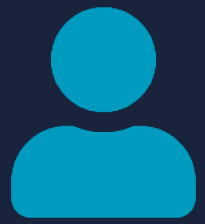




previder

it starts here.
it starts here.

MDR/ SIEM (SOC)



Gelukte inlogpoging
- Nieuw IP-Adres
- Verdachte locatie

SharePoint
- Items downloaden
- Items verwijderen
- Delen met derden

Response door SecOps

Suspicious MS365 activities

Analyse:
- Context IP-Adres
- Policy's: MFA wel vereist?
- Contact leggen met gebruiker
- Type bestanden (inhoud)
- Additionele processen / activiteiten

Maatregelen:
- Account blokkeren
- Wachtwoord vernieuwen
- Delen ongedaan maken
- IP blokkeren
- Contactpersoon informeren

previder

it starts here.
it starts here.

MDR/ SIEM (SOC)

Endpoint
- Verdacht netwerk activiteit
- Download software
- Malafide URL

Threat Intelligence
- IP-adres
- Hashes
- URL

Response door SecOps

Suspicious connectivity

Analyse:
- Context IP-Adres / hashfile
- Contact leggen met gebruiker
- Additionele processen / activiteiten
- Oorsprong achterhalen
- Verdere analyse / mogelijk vervolg

Maatregelen:
- Account blokkeren
- IP blokkeren
- Bestand verwijderen
- Device isoleren
- Contactpersoon informeren

previder

it starts here.
it starts here.

Tips bij MDR selectie

- Welke (rest) risico's wil ik reduceren?
- Welke kritische componenten in mijn infrastructuur wil ik monitoren?
- Heb ik MDR inclusief herstel nodig of besteed ik het uit/doen we zelf?

Bedankt voor jullie aandacht

previder

it starts here.